信息安全管理体系认证实施规则

文件编号：CECC-GZ-ISMS：2025 A/1

发布日期：2025年06月10日

实施日期：2025年06月10日

修订日期：2026年01月01日

1.总则

1.1 适用范围

本规则用于规范中电联（北京）检测认证中心 “以下简称 CECC”，对申请认证和获证的各类组织按照 GB/T22080《信息安全管理体系 要求及使用指南》标准建立信息安全管理体系的认证活动。

1.2 CECC 是认证活动的第一责任人，对本认证规则的合法性、合规性、真实性、完整性、科学性、适用性等负责，承担认证规则制定及实施的主体责任，并做出公开承诺。本认证规则符合以下原则：

1.2.1 不得与国家法律、行政法规、部门规章、行政规范性文件和政策规定相抵触。

1.2.2 不得与现行国家或地方相关行政许可规定相抵触。

1.2.3 不得与国家认监委制定或者会同国务院有关部门制定发布的认证基本规范、认证规则要求相抵触。

1.2.4 不得与现行相关强制性国家标准相抵触，鼓励高于国家标准、行业标准要求。

1.2.5 不违背社会公序良俗和社会公共利益。

1.2.6 在未经国家认监委统筹安排下，不备案涉及国家安全、政治组织、社会民俗、民族宗教等领域的认证规则。

1.2.7 不得违反知识产权、保密相关规定。

1.2.8 不混淆制定、备案和使用产品、服务和管理体系认证规则。

1.2.9 不违反全国统一大市场、公平竞争等原则要求。

1.2.10 不得违反国家认监委相关要求。

1.3 本规则是对 CECC 从事信息安全管理体系认证活动的基本要求，所有认证审核人员从事该项认证活动应当遵守本规则。

1.4 审核依据

GB/T22080《信息安全管理体系 要求及使用指南》

1.5 利益相关方

CECC 主要服务电力行业涉及的发电、供电、电力设计等国有大中型企业，与信息安全管理体系有关的相关方；

1.5.1 各相关方信息安全管理方面的需求和期望；

1.5.2 信息安全管理相关的合规义务要求。

1.5.3 确定管理体系的范围

电力企业应界定信息安全管理体系的边界和应用范围。确定该边界和范围时，组织应考虑：

a) IMS 4.1 中所提及的外部和内部问题；

b) IMS 4.2 中所提及的要求；

c) IMS 4.3 提及的组织单元、职能和物理边界；

d) 其活动、产品和服务；

e) 其权限和实施控制及影响的能力。

电力企业确定信息安全管理体系的边界和范围后，在该范围内组织的所有产品和服务涉及的信息安全风险均应纳入管理体系控制。若组织认为其信息安全管理体系的应用范围不适用本标准的某些要求，应说明理由。那些不适用的范围，不能影响电力企业信息安全管理体系运行合规义务和对相关方需求的满足，否则不能声称符合本标准。

2 CECC 资质要求

2.1 获得国家认监委批准、取得从事信息安全管理体系认证的资质。

2.2 建立可满足 GB/T 27021《合格评定 管理体系审核认证机构要求》的内部管理体系，以使从事的信息安全管理体系认证活动符合法律法规及技术标准的规定。

2.3 建立内部制约、监督和责任机制，实现受理、培训（包括相关增值服务）、审核和做出认证决定等环节的相互分开。

2.4 CECC 为通过认可机构的认可，从事的信息安全管理体系认证能力符合要求。

3 对认证人员的要求

3.1 认证人员应当取得国家认监委确定的认证人员注册机构颁发的信息安全管理体系审核员注册资格。

3.2 认证人员应当遵守与从业相关的法律法规，对认证活动及做出的认证审核报告和认证结论的真实性承担相应的法律责任。

3.3 认证人员能力管理

认证人员能力应满足 CNAS-CC170：2015 信息安全管理体系认证机构要求

第 7 章人员能力要求。为确保中心所有参与审核和认证活动的人员都能满足预期结果，对认证评定人员的能力和表现进行复核，并识别培训要求，CECC 采用多种方式并在考虑了审核人员有能力实施不同认证制度管理体系类型的情况进行监视和测量。这些方式包括：

（1）日常信息（客户反馈、表扬、投诉）；

（2）审核报告复核及审核资料检查；

（3）定期对审核员进行现场见证，其频次根据使用的频率、承担审核项目的风险程度和个人表现，包括负面反馈而定；

（4）审核员年度综合评价。

具体的监视及现场见证要求，详见 CECC《审核人员能力监视和再评价程序》。

3.4 外部审核员和技术专家的使用

CECC 的审核员、技术专家分为专职和兼职，兼职的审核员和技术专家均属于外部人员。

3.4.1 CECC 对于外部人员的使用做出如下规定：

3.4.1.1 以书面协议的方式，确保外部人员承诺遵守本中心的公正性政策并按照中心的规定实施相关过程，包括保密及公正性的管理规定；

3.4.1.2 有程序确保所使用兼职审核员和技术专家能够向 CECC 说明现在或以前与可能派其审核的组织的关系；

CECC 的相关程序文件同样适用于外部人员的管理和监控。

4 初次认证程序

4.1 受理认证申请

4.1.1 CECC 应向申请认证的组织（以下简称申请组织）至少公开以下信息：

（1）可开展认证业务的范围，以及获得认可的情况。

（2）CECC 的授予、保持、扩大、更新、缩小、暂停或撤销认证及其证书等环节的制度规定。

（3）认证证书样式。

（4）对认证决定的申诉程序。

（5）分支机构和办事机构的名称、业务范围、地址等。

4.1.2 申请组织提交以下资料：

（1）认证申请书，包括申请组织的生产经营或服务活动等情况的说明。

（2）具有法律地位的证明文件（包括：企业营业执照、事业单位法人证书、社会团体体登记证书、非企业法人登记证书、党政机关设立文件等）的复印件。若信息安全管理体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）。

（3）具有组织机构代码证书的复印件。

（4） 信息安全管理体系覆盖的活动所涉及法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件。 必要时提供涉密等合规性文件。

（5）多场所活动、活动分包情况。

（6）信息安全管理体系手册及必要的程序文件。

（7）信息安全管理体系涉及的法律法规和其他要求的清单。

（8）信息安全管理体系已有效运行 3 个月以上的证明材料。

（9）其他与认证审核有关的必要文件。

4.1.3 认证申请的审查确认

CECC 应对申请组织提交的申请资料进行审查，并确认：

（1）申请资料齐全。

（2）申请组织从事的活动符合相关法律法规的规定。

（3）申请组织为达到信息安全目标而建立了文件化的信息安全管理体系。

4.1.4 根据申请组织申请的认证范围、生产经营场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

4.1.5 对符合 4.1.3、4.1.4 要求的，CECC 可决定受理认证申请；对不符合上述要求的，CECC 应通知申请组织补充和完善，或者不受理认证申请。

4.1.6 CECC 应完整保存认证申请的审查确认工作记录。

4.1.7 签订认证合同在实施认证审核前，CECC 应与申请组织订立具有法律效力的书面认证合同，合同应至少包含以下内容：

4.1.7.1 申请组织获得认证后持续有效运行信息安全管理体系的承诺。

4.1.7.2 申请组织对遵守认证认可相关法律法规，协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺。

4.1.7.3 申请组织承诺获得认证后发生以下情况时，应及时向 CECC 通报：

（1）相关方有重大投诉。

（2）发生职业健康安事故被执法监管部门认定为严重不符合法定要求。

（3）发生较大及以上信息安全事故未完成处置的。

（4）相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格、强制性认证或其他资质证书变更；法定代表人、最高管理者、管理者代表变更；生产经营或服务的工作场所变更；信息安全管理体系覆盖的活动范围变更；信息安全管理体系和重要过程的重大变更等。

（5）出现影响信息安全管理体系运行的其他重要情况。

4.1.7.4 申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息；不擅自利用信息安全管理体系认证证书和相关文字、符号误导公众认为其产品或服务通过信息安全认证。

4.1.7.5 拟认证的信息安全管理体系覆盖的生产或服务的活动范围。

4.1.7.6 在认证审核及认证证书有效期内各次监督审核中，CECC 和申请组织各自应当承担的责任、权利和义务。

4.1.7.8 认证服务的费用、付费方式及违约条款。

4.2 制定审核计划

4.2.1 审核时间

4.2.1.1 为确保认证审核的完整有效，CECC 应以附录 A 所规定的审核时间为基础，根据申请组织信息安全管理体系覆盖的活动范围、特性、信息安全风险程度、认证要求和员工人数等情况，核算并拟定完成审核工作需要的时间。在特殊情况下，可以减少审核时间，但减少的时间不得超过附录 A 所规定的审核时间的 30 %。

4.2.1.2 整个审核时间中，现场审核时间不应少于 80%。

4.2.1.3 详细计算详见附录 A 说明。

4.2.2 审核组

4.2.2.1 CECC 应当根据信息安全管理体系覆盖的活动的专业技术领域选择具备相关能力的审核员和技术专家组成审核组。审核组中的审核员应承担审核责任。

4.2.2.2 技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

4.2.2.3 审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，在审核过程中的活动由审核组中的审核员承担责任。

4.3 实施审核

4.3.1 审核方案

4.3.1.1 CECC 依据 GB/T19011、CANS 105、CANS 11 等规范要求对整个认证周期制定审核方案，审核方案应覆盖全部的管理体系要求，并符合下述规定：

（1）包括两个阶段初次审核，认证决定之后的第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核；

（2）三年的认证周期从初次认证决定或再认证决定算起；

（3）审核方案的确定和任何后续调整应考虑客户的规模，其管理体系、产品和过程范围与复杂程度，以及经过证实的管理体系有效性水平和以前的审核结果；

明确审核项目特定能力的需求，包括涉及技术领域的专业能力，专业能力包括与客户组织的信息安全管理风险、信息安全设施、设备、系统和过程的特点相关的能力；

基于客户管理体系文件界定的管理体系边界与范围的信息，确定“审核范围”，以便审核策划；包括多场所的抽样方案。

4.3.1.2 建立审核方案的活动包括：

（1）确定审核方案的目的；

（2）确定审核方案的内容要考虑审核应覆盖的区域和单元、审核频次、采用准则、每一审核应覆盖的活动等；

（3）明确审核方案的职责；

（4）确定资源；

（5）确定程序，应明确实施和监视审核方案的方式：

审核策划和日程安排；

保证审核员和审核组长的能力；

选择适当的审核组并分配其任务和职责；

实施审核；

实施审核后续活动；

保持审核方案的记录；

监视审核方案的业绩和有效性；

向最高管理者报告审核方案的总体实现情况；

4.3.1.3 监督审核的频次及时机

监督审核应至少每个日历年（应进行再认证的年份除外）进行一次。初次认证后的第一次监督审核应在认证决定日期起 12 个月内进行；

在策划监督审核的频次和时机时，应注意了解受审核方业务运作的时间(季节或有限时段)特点，并了解客户内部审核方案安排的情况，合理选取和安排监督审核的周期及具体实施的时间；

出于认证行业公信力的需要，CECC 将自觉遵守认证监管部门对于监督频次的特定要求。

4.3.1.4 如果客户已获的认证或由另一个认证机构实施的审核，则应获取并保留充足的证据，如审核报告、不符合报告及相应的纠正措施文件等，所获取的文件应能够证明对审核方案任何调整的合理性，并予以记录，并对以前不符合的纠正措施的实施情况进行跟踪验证，具体执行 CNAS CC12 的管理规定。

4.3.1.5 如果客户采用连续作业，应在建立审核方案和编制审核计划时考虑在连续作业不同作业环境的审核安排。

4.3.1.6 审核管理处是审核方案的策划部门，并负责对于审核方案的实施情况进行监视以及结果的评价和改进工作。

4.3.2 审核计划

4.3.2.1 CECC 应制定书面的审核计划交审核组实施。审核计划至少包括以下内容：审核目的、审核范围、审核过程、审核涉及的部门和场所、审核时间、审核组 成员（其中：审核员应标明注册证书号及专业代码；技术专家应标明专业代码、技术职称或职务，如果在职应注明其服务的单位）。

4.3.2.2 通常情况下，初次认证审核、监督审核和再认证审核应在申请组织申请认证的范围涉及到的各个场所现场进行。如果信息安全管理体系包含在多个场所进行相同或相近的活动，且这些场所都处于该申请组织授权和控制下，CECC 可以在审核中对这些场所进行抽样，但应制定合理的抽样方案以确保对各场所信息安全管理体系的正确审核。如果不同场所的活动存在根本不同、或不同场所存在

可能对信息安全管理产生显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

4.3.3.3 为使现场审核活动能够观察到产品生产或服务活动情况产生的信息安全风险，现场审核应安排在认证范围覆盖的产品生产或服务活动正常运行时进行。

4.3.3.4 在审核活动开始前，审核组应将书面审核计划交申请组织确认。遇特殊情况临时变更计划时，应及时将变更情况书面通知受审核的申请组织，并协商一致。

4.3.2 审核组应当全员完成审核计划的全部工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员（技术专家和实习审核员除外）。

4.3.3 审核组应当会同申请组织按照程序顺序召开首、末次会议。审核组应当提供首、末次会议签到表，参会人员应签到。

4.3.4 审核过程及环节

4.3.4.1 初次认证审核，分为第一、二阶段实施审核。

4.3.4.2 第一阶段审核应至少覆盖以下内容：

（1）结合现场情况，确认申请组织实际情况与信息安全管理体系文件描述的一致性， 特别是体系文件中描述的产品或服务、部门设置和负责人、生产或服务过程等是否与 申请组织的实际情况相一致。

（2）结合现场情况，审核申请组织有关人员理解和实施 GB/T 124001/ISO14001 标准要求的情况，评价信息安全管理体系运行过程中是否实施了内部审核与管理评审，确认信息安全管理体系是否已有效运行并且超过 3 个月。 对信息安全管理体系文件不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的，应当及时终止审核。

（3）确认申请组织建立的信息安全管理体系覆盖的活动内容和范围、申请组织的员工人数、活动过程和场所，遵守相关法律法规及技术标准的情况。

（4）结合信息安全管理体系覆盖活动的特点识别对信息安全目标的实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点。

（5）与申请组织讨论确定第二阶段审核安排。

4.3.3.3 在下列情况，第一阶段审核可以不在申请组织现场进行：

（1）申请组织已获本 CECC 颁发的其他认证证书，CECC 已对申请组织职业健康

管理体系有充分了解。

（2）CECC 有充足的理由证明申请组织的生产经营或服务的技术特征明显、过程简单、信息安全风险较低，通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求。

（3）申请组织获得过其他经认可的认证机构颁发的有效的信息安全管理体系认证证书，通过对其文件和资料的审查可以达到第一阶段审核的目的和要求。除以上情况之外，第一阶段审核应在申请组织的生产经营或服务现场进行。

4.3.3.4 审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注。

4.3.3.5 第一阶段审核和第二阶段审核应安排适宜的间隔时间，使申请组织有充分的时间解决第一阶段中发现的问题。

4.3.3.6 第二阶段审核应当在申请组织现场进行。重点是审核信息安全管理体系符合 GB/T22080/ISO/IEC27001 标准要求和有效运行情况，应至少覆盖以下内容：

（1）在第一阶段审核中识别的重要审核点的信息安全运行、监视、测量、报告和评审记录的完整性和有效性。

（2）为实现总信息安全目标而建立的各层级目标是否具体、有针对性、可测量并且可实现。

（3）对信息安全管理体系覆盖的过程和活动的管理及控制情况。

（4）申请组织实际工作记录是否真实。

（5）申请组织的内部审核和管理评审是否有效。

4.3.4 发生以下情况时，审核组应终止审核，并向 CECC 报告。

4.3.4.1 申请组织对审核活动不予配合，审核活动无法进行。

4.3.4.2 申请组织的信息安全管理体系有重大缺陷，不符合 GB/T22080/ISO/IEC27001 标准的要求。

4.3.3.3 发现申请组织存在重大环境安全问题或有其他严重违法违规行为。（4）其他导致审核程序无法完成的情况。

4.4 审核报告

4.4.1 审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

（1）申请组织的名称和地址。

（2）审核的申请组织活动范围和场所。

（3）审核组组长、审核组成员及其个人注册信息。

（4）审核活动的实施日期和地点。

（5)叙述从 4.3 条列明的程序及各项要求的审核工作情况，其中：对 4.3.3.6 条的各项审核要求应逐项就审核证据、审核发现和审核结论进行详细描述；对信息安全目标实现情况的评价，应同时叙述测量方法。

（6）识别出的不符合项。不符合项的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被申请组织理解。不得用概念化的、不确定的、 含糊的语言表述不符合项。

（7）审核组对是否通过认证的意见建议。

4.4.2 审核报告应随附必要的用于证明相关事实的证据或记录，包括文字或照片摄像等音像资料。

4.4.3 CECC 应将审核报告提交申请组织，并保留签收或提交的证据。

4.4.4 对终止审核的项目，审核组应将已开展的工作情况形成报告，CECC 应 将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

4.5 不符合项的纠正和纠正措施及其结果的验证

4.5.1 对审核中发现的不符合项，CECC 应要求申请组织分析原因，并要求申 请组织在规定期限内采取措施进行纠正。

4.5.2 CECC 应对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。

4.6 认证决定

4.6.1 CECC 应该在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，做出认证决定。

4.6.2 审核组成员不得参与对审核项目的认证决定。

4.6.3 CECC 在做出认证决定前应确认如下情形：

4.6.3.1 审核报告符合本规则第 4.4 条要求，能够满足做出认证决定所需要的信息。

4.6.3.2 反映以下问题的不符合项，CECC 已评审、接受并验证了纠正和纠正措 施及其结果的有效性。

（1）未能满足信息安全管理体系标准的要求。

（2）制定的信息安全目标不可测量、或测量方法不明确。

（3）对实现信息安全目标具有重要影响的处置措施、关键点的监视和测量未有效运行，或者对这些处置措施、关键点的报告或评审记录不完整或无效。

（4）在持续改进信息安全管理体系的有效性方面存在缺陷，实现信息安全目标有重**大疑问。**

4.6.3.3 CECC 对其他不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

4.6.4 在满足 4.6.3 条要求的基础上，CECC 有充分的客观证据证明申请组织 满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书。

4.6.4.1 申请组织的信息安全管理体系符合标准要求且运行有效。

4.6.4.2 认证范围覆盖的产品或服务符合相关法律法规要求。

4.6.4.3 申请组织按照认证合同规定履行了相关义务。

4.6.5 申请组织不能满足上述要求的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

4.6.6 CECC 在颁发认证证书后，应当在 30 个工作日内按照规定的要求将相关信息报送国家认监委。国家认监委在其网站（www.cnca.gov.cn）专栏向社会公开 CECC 上报的认证证书等信息。

4.6.7 CECC 不得将申请组织是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

5 监督审核程序

5.1 CECC 应对持有其颁发的信息安全管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织通过认证的信息安全管理体系持续符合要求。

5.2 为确保达到 5.1 条要求，CECC 应根据获证组织的产品或服务的信息安全风险程度或其他特性，确定对获证组织的监督审核的频次。

5.2.1 作为最低要求，在初次认证的第二阶段审核后至少 12 个月内应进行一次监督审核。此后，每次监督审核的时间间隔不超过 12 个月。

5.2.2 在达到监督审核期限而有证据表明获证组织暂不具备实施监督审核的条件时，可以适当延长监督审核期限，但最长间隔不能超过 15 个月。

5.2.3 超过期限而未能实施监督审核的，应按 7.2 或 7.3 条处理。

5.3 监督审核的时间，应不少于按 4.2.1 条计算审核时间人日数的 30%。

5.4 监督审核的审核组，应符合 4.2.2 条和 4.3.1 条的要求。

5.5 监督审核应在获证组织现场进行，且应满足第 4.2.3.3 条确定的条件。由于产品生产的季节性原因，在每次监督审核时难以覆盖所有产品的，在认证证书有效期内的监督审核需覆盖认证范围内的所有产品和服务。

5.6 监督审核时至少应审核以下内容：

5.6.1 ISMS 在实现客户信息安全方针的目标方面的有效性；

5.6.2 对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

5.6.3 所确定的控制的变更，及其引起的 SoA 的变更；

5.6.4 控制的实施和有效性（根据审核方案来审查）。

5.6.5 CECC 应能够针对与信息安全问题相关的风险及其对客户的影响来调整监督方案，并说明监督方案的合理性。 监督审核可以与其他管理体系的审核相结合。报告应清晰地指出与每个管理体系相关的方面。

5.6.7 在监督审核过程中，CECC 应检查客户提交给认证机构的申诉和投诉记录，并且在发现任何不符合或不满足认证要求时，还应检查客户是否对其自身的 ISMS 和规程进行了调查并采取了适当的纠正措施。 特别是，监督报告应包括有关消除以往出现的不符合、SoA 版本和从上次审核之后发生的重大变更的信息。

5.6.8 信息安全目标及各层级信息安全目标是否实现。目标没有实现的，获证组织在内部管理评审时是否及时调查并采取了改进措施。

5.6.9 获证组织对认证标志的使用或对认证资格的引用是否符合相关的规定。

5.6.10 内部审核和管理评审是否规范和有效。

5.6.11 是否及时接受和处理投诉。

5.6.12 针对内审发现的问题或投诉的问题，及时制定并实施了有效的持续改进。

5.7 监督审核的审核报告，应按 5.6 条列明的审核要求逐项描述审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议。

5.8 CECC 根据监督审核报告及其他相关信息，做出继续保持或暂停、撤销认证证书的决定。

中电联（北京）检测认证中心有限责任公司

CEC (Beijing) Testing & Certification Center Co.,Ltd.

信息安全管理体系认证证书

注册号：

获证企业名称：

企业注册地址：

统一社会信用代码：

标准编号：

认证范围：

原发证日期：　　总经理签字：

换证日期：

证书有效期：

电力认证

本证书的有效性是通过年度监督检查得到的保持，请按以下方式查询核实:国家认监委网站http://www.cnca.gov.cn/;

本中心网址：www.cecc.com.cn；本中心电话：010-8393 5893.

地址:北京市丰台区槐房西路9号院7号楼8层801-1　邮编:100076