EWC-R- PIIpMS：2020

基于 ISO/IEC 29151 的个人信息安全管理体系认证规则

北京埃尔维质量认证中心

目　　录

基于ISO/IEC 29151的个人信息安全管理体系认证规则

1适用范围

1.1 本规则用于规范北京埃尔维质量认证中心（以下简称EWC）依据ISO/IEC 29151:2017 《Information Technology-Security Techniques-Code of Practice for Personally Identifiable Information Protection信息技术－安全技术－个人可识别信息保护实践指南》开展的基于ISO29151的个人信息安全管理体系认证规则

1.2 本规则旨在依据认证认可相关法律法规和技术标准的要求，对基于ISO29151的个人信息安全管理体系认证规则实施过程作出具体规定，明确EWC对认证过程的管理责任，保证基于ISO29151的个人信息安全管理体系认证规则活动的规范有效。

1.3 本规则是EWC及受审核方与获证组织在基于ISO29151的个人信息安全管理体系认证活动中的基本要求，认证双方在该项认证活动中应当遵守本规则。

2 主要依据文件

(1) ISO/IEC 29151：2017 《Information Technology-Security Techniques-Code of Practice for Personally Identifiable Information Protection》信息技术－安全技术－个人可识别信息保护实践指南

(2) CNAS-CC01:2015《管理体系认证机构要求》;

(3) IAF 强制性文件

(4) ISO 19011:2011 管理体系审核指南;

3 认证依据标准

ISO/IEC 29151：2017 《Information Technology-Security Techniques-Code of Practice for Personally Identifiable Information Protection》信息技术－安全技术－个人可识别信息保护实践指南

4 对 EWC 的要求

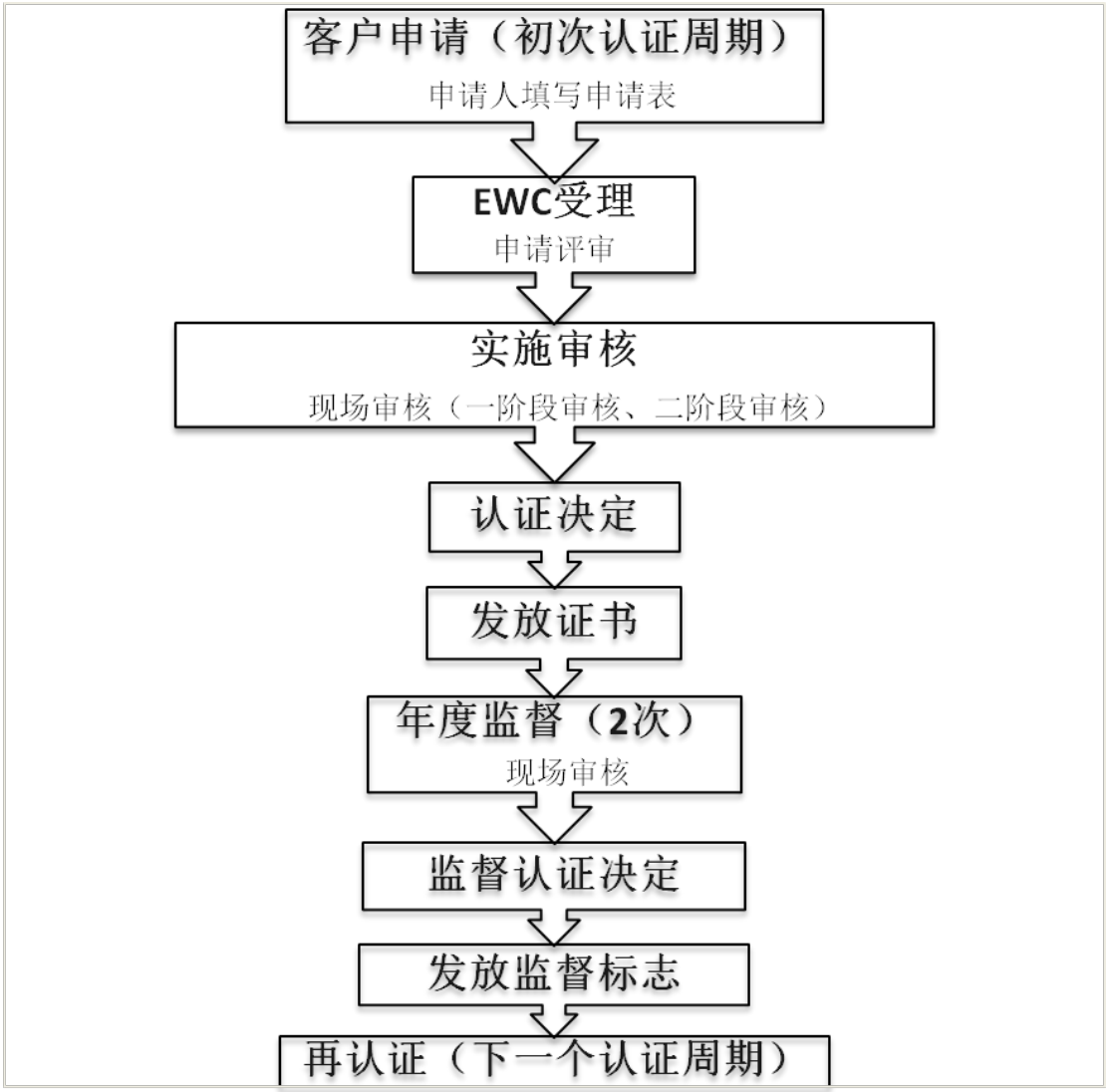
4.1 本认证规则发布、更新、撤销后，30日内向国家认监委备案。

4.2 建立可满足GB/T 27021/ISO/IEC 17021-1《合格评定 管理体系审核EWC要求》的内部管理体系，以使从事的基于ISO29151的个人信息安全管理体系认证活动符合相关法律法规及技术标准的规定。

4.3 建立内部制约、监督和责任机制，实现培训(包括相关增值服务)、审核和作出认证决定等环节的相互分开，以确保认证审核的公正性。

4.4 适时申请通过认可机构的认可，证明其从事的基于ISO29151的个人信息安全管理体系认证能力符合要求。

4.5 认证流程



5 对认证人员的要求

5.1 基于ISO29151的个人信息安全管理体系审核员应当取得国家认监委确定的认证人员注册机构颁发的ISMS或ITSMS管理体系审核员注册资格。

5.2 认证审核员完成相应的基于ISO29151的个人信息安全管理体系培训，并考核合格。

5.3 认证人员应当遵守与从业相关的法律法规，对认证活动及作出的

认证审核报告和认证结论的真实性承担相应的法律责任。

5.4 申请方/受审核方的义务

(1) 按本中心要求提交申请文件及其附件；

(2) 为本中心提供保证审核工作顺利进行必要的食、宿、行及办公条件；

(3) 为本中心审核组进入审核区域、调阅文件记录、安排被访问人员等提供必要的条件；适用时，为接纳到场的观察员（如认可机构评审员）提供条件。

(4) 保留顾客和/或相关方就获证组织的活动、产品或服务所提出的所有投诉记录，信息沟通记录及相应纠正措施记录，并在本中心要求时提供。重要投诉应及时通报赛宝认证中心。

(5) 按规定及时交纳认证费用。

6 初次认证程序

6.1 认证申请

6.1.1 申请的基本条件

1) 中国企业持有工商行政管理部门颁发的《企业法人营业执照》、《生产许可证》或等效文件；外国企业持有关机构的登记注册证明。

2) 申请方的基于 ISO29151 的个人信息安全管理体系已按 ISO/IEC 29151 标准的要求建立，并实施运行 3 个月以上。

3) 至少完成一次内部审核，并进行了管理评审。

4)基于 ISO29151 的个人信息安全管理体系运行期间及建立体系前的一年内未受到主管部门行政处罚。

6.1.2EWC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。

（2）本机构的授予、拒绝、保持、扩大、更新、缩小、暂停、恢复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）对认证过程的申投诉规定。

（5）分支机构和办事机构的名称、业务范围、地址等。

6.1.3申请组织应向EWC提交以下资料：

（1）认证申请书。

（2）法律地位的证明文件（如：企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等）的复印件。若基于 ISO29151 的个人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）基于 ISO29151 的个人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。

（4）多场所活动、活动分包情况 （适用时）。

（5）相关基于 ISO29151 的个人信息安全管理体系文件化信息(适用时)。

6.1.4EWC应确认申请资料是否齐全，并对申请组织提交的申请资料进行审查。

6.1.5EWC应根据申请组织申请的认证范围、生产经营和服务场所、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。审核时间的计算见附录A，PIIpMS认证业务范围采用信息安全管理体系认证业务分类表。

6.1.6对符合6.1.3、6.1.4要求的，EWC可决定受理认证申请；对不符合上述要求的，EWC应通知申请组织补充和完善，或者不受理认证申请。

6.1.7EWC应完整保存认证申请的审查确认工作记录。

6.1.8签订认证合同

在实施认证审核前，EWC 将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：

（1）申请组织获得认证后持续有效运行基于 ISO29151 的个人信息安全管理体系的承诺。

（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。

（3）申请组织承诺获得认证后发生以下情况时，应及时向 EWC 通报：

①发生产品和服务的基于 ISO29151 的个人信息安全事故。

②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、主要联系人变更；基于 ISO29151 的个人信息安全管理体系覆盖的活动范围变更；基于 ISO29151 的个人信息安全管理体系和重要过程的重大变更等。

③出现影响基于 ISO29151 的个人信息安全管理体系运行的其他重要情况。

（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；不擅自利用基于 ISO29151 的个人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和服务通过认证。

（5）拟认证的基于 ISO29151 的个人信息安全管理体系覆盖的生产或服务的活动范围。

（6）在认证审核实施过程及认证证书有效期内，EWC 和申请组织各自应当承担的责任、权利和义务。

（7）认证服务的费用、付费方式及违约条款。

6.2 审核策划

6.2.1审核时间

6.2.1.1为确保认证审核的完整有效，EWC根据申请组织基于ISO29151的个人信息安全管理体系覆盖的活动范围、环境背景和风险、组织规模等情况，核算并拟定完成审核工作需要的时间。附录A给出了确定审核时间的指南，业务范围采用信息安全管理体系认证业务分类表。

6.2.1.2整个审核时间中，现场审核时间不应少于总人日数的80％。

6.2.2审核组

6.2.2.1EWC应当根据基于ISO29151的个人信息安全管理体系覆盖的活动的行业领域选择具备相关能力的审核员和（或）技术专家组成审核组。审核组中的审核员应承担审核责任。

6.2.2.2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。

6.2.2.3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，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

6.2.3审核计划

6.2.3.1审核前应制定书面的审核计划。审核计划至少包括以下内容：审核目的、审核准则、审核范围、审核涉及的过程、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相关专业代码；技术专家应标明专业代码）。

6.2.3.2初次认证审核、监督审核和再认证审核应在受审核方申请认证的范围涉及到的场所现场进行。

如果基于 ISO29151 的个人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受审核方授权和控制下，EWC 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基于 ISO29151 的个人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基于

ISO29151 的个人信息安全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。

6.2.3.3为使现场审核活动能够观察到产品生产或服务活动情况，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，并考虑轮班作业班次安排。

6.2.3.4在审核活动开始前，审核组应将书面审核计划交受审核方确认。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受审核方，并协商一致。

6.3 实施审核

6.3.1审核组应当按照审核计划的安排完成审核工作。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）。

6.3.2审核组应当会同受审核方按照程序顺序召开首、末次会议，参会人员应签到。审核组应当提供首、末次会议签到表。参会人员应签到。受审核方要求时，审核组成员应向受审核方出示身份证明文件。

6.3.3审核过程及环节

6.3.3.1初次认证审核，分为第一、二阶段实施审核。

6.3.3.2第一阶段审核应至少覆盖以下内容：

（1）结合现场情况，确认受审核方实际情况与基于 ISO29151 的个人信息安全管理体系文件化信息描述的一致性。

（2）结合现场情况，审核受审核方有关人员理解和实施 ISO/IEC

29151 标准要求的情况，评价基于 ISO29151 的个人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。

对基于 ISO29151 的个人信息安全管理体系文件化信息不符合现场实际,以及其他不具备二阶段审核条件的,应当不实施二阶段审核。

（3）确认受审核方建立的基于 ISO29151 的个人信息安全管理体系覆盖的活动内容和范围、活动过程和场所，遵守适用的法律法规及强制性标准的情况。

（4）结合基于 ISO29151 的个人信息安全管理体系覆盖产品和服务的特点识别对基于 ISO29151 的个人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）与受审核方讨论确定第二阶段审核安排。

6.3.3.3在下列情况，第一阶段审核可以不在受审核方现场进行，但应记录未在现场进行的原因：

（1）受审核方已获本 EWC 颁发的其他有效认证证书，EWC 已对受审核方基于 ISO29151 的个人信息安全管理体系有充分了解。

（2）受审核方获得了其他经认可的 EWC 颁发的有效的基于 ISO29151 的个人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，第一阶段审核应在受审核方的生产经营或服务现场进行。

6.3.3.4审核组应将第一阶段审核情况形成书面文件告知受审核方。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

醒受审核方特别关注。

6.3.3.5第一阶段审核和第二阶段审核应安排适宜的间隔时间，使受审核方有充分的时间解决第一阶段中发现的问题。

6.3.3.6第二阶段审核应当在受审核方现场进行。重点是审核基于ISO29151的个人信息安全管理体系符合ISO/IEC 29151 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（关键过程）控制的有效性。

（2）为实现基于 ISO29151 的个人信息安全方针而在相关职能、层次和过程上建立基于 ISO29151 的个人信息安全目标是否具体适用、可测量并得到沟通、监视。

（3）对基于 ISO29151 的个人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）受审核方的内部审核和管理评审是否有效。

（5）受审核方实际运行记录的真实性等。

6.3.4发生以下情况时，审核组应向EWC报告，经EWC评议同意后，终止审核。

（1）受审核方对审核活动不予配合，审核活动无法进行。

（2）受审核方的基于 ISO29151 的个人信息安全管理体系有重大缺陷，不符合 ISO/IEC 29151 标准的要求。

（3）发现受审核方存在重大基于 ISO29151 的个人信息安全问题或有其他与产品和服务基于 ISO29151 的个人信息安全相关严重违法

违规行为。

（4）其他导致审核程序无法完成的情况。

6.4 审核报告

6.4.1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）受审核方的名称和地址。

（2）审核的受审核方活动范围和场所。

（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，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

（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描述或引用审核证据、审核发现和审核结论；对基于 ISO29151 的个人信息安全目标和过程及基于 ISO29151 的个人信息安全绩效实现情况进行评价。

（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，易于被受审核方理解。

（7）审核组对是否通过认证的意见建议。

（8）关于管理体系符合性与有效性的声明以及对下列方面相关

证据的总结：

①管理体系满足适用要求和实现预期结果的能力；

② 内部审核和管理评审的过程。

(9) 对认证范围适宜性的结论。

(10) 确认是否达到审核目的。

6.4.2EWC应保留用于证实审核报告中相关信息的证据。

6.4.3EWC应在作出认证决定后30个工作日内将审核报告提交受审核方，并保留签收或提交的证据。

6.4.4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，EWC应将此报告及终止审核的原因提交给受审核方，并保留签收或提交的证据。

6.5 不符合项的纠正和纠正措施及其结果的验证

6.5.1所有纠正措施应在审核组与受审方商定的时限内完成并经审核组验证，最长时限不超过90天。超出此期限，EWC保留重新实施一次第二阶段审核的权利。当审核期间发现客户组织存在严重不符合，审核组长现场与客户组织相关人员就严重不符合的性质、影响的范围等协商整改的时间限制，以避免可能造成的损失。如果客户组织未能在协商的时间内完成严重不符合实施的纠正和纠正措施，并由审核组成员验证有效，则EWC保留推荐认证前再次实施一次第二阶段审核的权利。

6.5.2EWC应对受审核方所采取的纠正和纠正措施及其结果的有效性

进行验证。

6.6 认证决定

6.6.1EWC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，作出认证决定并保持认证决定记录。

6.6.2认证决定人员应为EWC管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

6.6.3EWC在作出认证决定前应确认如下情形：

（1）审核报告符合本规则第 6.4 条要求，能够满足作出认证决定所需要的信息。

（2）反映以下问题的不符合项，EWC 已评审、接受并验证了纠正和纠正措施的有效性。

①在持续改进基于 ISO29151 的个人信息安全管理体系的有效性方面存在缺陷，实现基于 ISO29151 的个人信息安全目标有重大疑问。

②制定的基于 ISO29151 的个人信息安全目标不可测量、或测量方法不明确。

③对实现基于 ISO29151 的个人信息安全目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效。

④其他严重不符合项。

（3）EWC 对其他一般不符合项已评审，并接受了受审核方计划采取的纠正和纠正措施。

6.6.4在满足6.6.3条要求的基础上，EWC有充分的客观证据证明受审核方满足下列要求的，评定该受审核方符合认证要求，向其颁发认证证书。

（1）受审核方的基于 ISO29151 的个人信息安全管理体系符合标准要求且运行有效。

（2）认证范围覆盖的产品和服务符合相关法律法规要求。

（3）受审核方按照认证合同规定履行了相关义务。

6.6.5受审核方不能满足上述要求的，评定该受审核方不符合认证要求，以书面形式告知受审核方并说明其未通过认证的原因。

6.6.6EWC 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）开设专栏向社会公开各 EWC 上报的认证证书等信息。

6.6.7EWC不得将受审核方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。

7 监督审核程序

7.1EWC应对持有其颁发的基于ISO29151的个人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基于ISO29151的个人信息安全管理体系持续符合要求。

7.2为确保达到7.1条要求，EWC将根据获证组织的产品和服务的基于ISO29151的个人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。

7.2.1 作为最低要求，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。此后，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。

7.2.2 超过期限而未能实施监督审核的，应按9.2或9.3条处理。

7.3 监督审核的时间，应不少于按6.2.1条计算审核时间人日数的三分之一。

7.4 监督审核应在获证组织现场进行，且应满足第 6.2.3.3 条确定的条件。由于市场、季节性等原因，在每次监督审核时难以覆盖所有产品和服务的，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。

7.5 监督审核时至少应审核以下内容：

（1）上次审核以来基于 IS029151 的个人信息安全管理体系覆盖的活动及影响体系的重要变更及运行体系的资源是否有变更。

（2）按 6.3.3.2 条要求已识别的重要关键点是否按基于 IS029151 的个人信息安全管理体系的要求在正常和有效运行。

（3）对上次审核中确定的不符合项采取的纠正和纠正措施是否继续有效。

（4）基于 IS029151 的个人信息安全管理体系覆盖的产品和服务涉及法律法规规定的，是否持续符合相关规定。

（5）基于 IS029151 的个人信息安全目标及基于 IS029151 的个人信息安全绩效信息。基于 IS029151 的个人信息安全目标及绩效没

有实现的，获证组织是否及时调查并采取了改进措施。

（6）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。

（7）内部审核和管理评审是否规范和有效。

（8）是否及时接受和处理投诉。

（9）针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

7.6 监督审核的审核报告，应按 7.5 条列明的审核要求进行描述或引用审核证据、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。

7.7EWC 根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

8 再认证程序

8.1 认证证书期满前，若获证组织申请继续持有认证证书，EWC 将实施再认证审核，并决定是否延续认证证书。

8.2EWC 将派出审核组。按照 6.2.3 条要求并结合历次监督审核情况，制定再认证计划由审核组实施。审核组按照要求开展再认证审核。

在基于 ISO29151 的个人信息安全管理体系及获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段审核，但审核时间应不少于按 6.2.1 条计算人日数的 2/3。

当基于 ISO29151 的个人信息安全管理体系、组织管理机构或管

理体系的运作环境有重大变更时，EWC 将与受审核方充分沟通，判断是否需要进行一阶段审核，如不需要，应记录理由。

8.3 对再认证审核中发现的严重不符合项，EWC 应规定实施纠正与纠正措施的时限。验证应在原证书到期前完成。

8.4EWC 按照 6.6 条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

8.5 如果在原证书到期前，EWC 未能完成再认证审核或不能验证对严重不符合实施的纠正和纠正措施，则不应予以再认证，也不应延长认证的效力。

在认证到期后,如果EWC能够在6个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。证书的生效日期应不早于再认证决定日期,终止日期应基于上一个认证周期。

9 暂停或撤销认证证书

9.1EWC 应制定暂停、撤销认证证书或缩小认证范围的规定，并形成文件化的管理制度。EWC 对认证证书的暂停和撤销处理应符合其管理制度和本规则的规定，不得随意暂停或撤销认证证书。

9.2 暂停证书

9.2.1 获证组织有以下情形之一的，EWC 应在调查核实后的 5 个工作日内暂停其认证证书。

（1）基于 ISO29151 的个人信息安全管理体系持续或严重不满足

认证要求，包括对基于 ISO29151 的个人信息安全管理体系运行有效性要求的。

（2）不承担、履行认证合同约定的责任和义务的。

（3）被有关执法监管部门责令停业整顿的。

（4）被地方认证监管部门发现体系运行存在问题，需要暂停证书的。

（5）持有的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的。

（6）主动请求暂停的。

（7）其他应当暂停认证证书的。

9.2.2 认证证书暂停期不得超过 6 个月。但属于 9.2.1 第（5）项情形的暂停期可至相关单位作出许可决定之日。

9.2.3EWC 暂停认证证书的信息，应明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

9.3 撤销证书

9.3.1 获证组织有以下情形之一的，EWC 应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书。

（1）被注销或撤销法律地位证明文件的。

（2）拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的。

（3）出现重大基于 ISO29151 的个人信息安全事故，经执法监管

部门确认是获证组织违规造成的。

（4）有其他严重违反法律法规行为的。

（5）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）。

（6）没有运行基于 ISO29151 的个人信息安全管理体系或者已不具备运行条件的。

（7）不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者 EWC 已要求其纠正但超过 6 个月仍未纠正的。

（8）其他应当撤销认证证书的。

9.3.2 撤销认证证书后，EWC 应及时收回撤销的认证证书。若无法收回，EWC 应及时在相关媒体和网站上公布或声明撤销决定。

9.4EWC 暂停或撤销认证证书将在其网站上公布相关信息，同时按规定程序和要求报国家认监委。

9.5EWC 有义务和责任采取有效措施避免各类无效的认证证书和认证标志被继续使用。

10 认证证书要求

10.1 认证证书应至少包含以下信息：

（1）获证组织名称、地址和统一社会信用代码（或组织机构代码）。该信息应与其法律地位证明文件的信息一致。

（2）基于 ISO29151 的个人信息安全管理体系覆盖的生产经营或

服务的地址和业务范围。若认证的基于 ISO29151 的个人信息安全管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息。

（3)基于ISO29151的个人信息安全管理体系符合ISO/IEC 29151标准的表述，适用时，包括明示不适用的标准条款。

（4）证书编号。

（5）EWC 名称。

（6）证书签发日期及有效期的起止年月日。

证书将注明 “证书的有效性需经 EWC 沟通定期的监督审核确定保持”的提示信息。

（7）相关的认可标识及认可注册号（适用时)。

（8）证书查询方式。EWC 除公布认证证书在本机构网站上的查询方式外，还应当在证书上注明:“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询”，以便于社会监督。

10.2 初次认证认证证书有效期最长为 3 年。再认证证书的终止日期可以基于原认证证书的终止日期。

10.3EWC 将当建立证书信息披露制度。除向受审核方、认证监管部门等执法监管部门提供认证证书信息外,还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

11 与其他管理体系的结合审核

11.1 对基于 ISO29151 的个人信息安全管理体系和其他管理体系实施

结合审核时，通用或共性要求应满足本规则要求，审核报告中应清晰地体现 4.4 条要求，并易于识别。

11.2 结合审核的审核时间人日数，不得少于多个单独体系所需审核时间之和的 80%。

12 受理组织的申诉

受审核方或获证组织对认证决定有异议时，EWC 应接受申诉并且及时进行处理，在 60 日内将处理结果形成书面通知送交申诉人。

书面通知应当告知申诉人，若认为 EWC 未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

13 认证记录的管理

13.1EWC 应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

13.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间至少应当与认证证书有效期一致。

13.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式。

13.4 所有具有相关人员签字的记录，原件必须妥善保存，保存时间至少应当与认证证书有效期一致。

14 收费说明

EWC 应严格执行国家有关主管部门的收费规定。

15 其他

15.1 本规则内容提及 ISO/IEC 29151 标准时均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

15.2EWC 可开展基于 ISO29151 的个人信息安全管理体系及相关技术标准的宣贯培训,促使组织的全体员工正确理解和执行基于 ISO29151 的个人信息安全管理体系标准,但不得针对特定的组织提供具体的解决方案。

15.3 本规则的发布日期为 2020 年 3 月 15 日。

附录 A（资料性附录）

审 核 时 间

基于ISO29151的个人信息安全管理体系的审核时间与信息安全管理体系的审核时间相同。

若申请方已获得GB/T 22080(ISO/IEC 27001,IDT)有效认证证书，并且范围覆盖了基于ISO29151的个人信息安全管理体系申请范围，则基于ISO29151的个人信息安全管理体系的审核时间数按照信息安全管理体系的审核时间的0.5 倍+1天进行计算（向上取整至0.5人天），当GB/T 22080(ISO/IEC 27001,IDT)证书由北京埃尔维质量认证中心颁发时，则基于ISO29151的个人信息安全管理体系的审核时间数按照信息安全管理体系的审核时间的0.5 倍进行计算（向上取整至0.5人天）。

基于 ISO29151 的个人信息安全管理体系与信息安全管理体系结合审核时，审核时间按照信息安全管理体系的审核时间的 0.4 倍进行计算（向上取整至 0.5 人天）。