



EWC-R-PIIcISMS:2025

基于 ISO/IEC 27018 的公有云个人 信息安全管理 体系认证规则

2025-06-01 发布

2025-06-01 实施

北京埃尔维质量认证中心

目 录

1 适用范围.....	2
2 引用文件.....	2
3 认证依据.....	2
4 EWC 认证管理要求.....	2
5 申请方/受审核方的义务.....	3
6 认证实施程序.....	4
6.1 认证流程.....	4
6.2 认证申请与评审.....	4
6.3 审核策划.....	6
6.4 初次审核.....	7
6.5 审核报告.....	9
6.6 不符合项的纠正和纠正措施及其结果的验证.....	9
6.7 认证决定.....	10
6.8 监督审核程序.....	10
6.9 再认证程序.....	11
7 认证证书状态管理.....	12
8 认证证书要求.....	13
9 与其他管理体系的结合审核.....	14
10 组织的申诉及投诉.....	14
11 认证记录的管理.....	15
12 其他.....	15
附录 A（规范性附录）.....	16

基于 ISO/IEC 27018 的公有云个人 信息安全管理体系统认证规则

1 适用范围

1.1 本规则用于北京埃尔维质量认证中心（以下简称EWC）依据ISO/IEC 27018：2019《信息技术 安全技术 个人信息身份信息处理者在公有云中保护个人身份信息的实践指南》标准及本认证规则开展的公有云个人信息安全管理体系认证活动。

1.2 本规则旨在依据认证相关法律法规和技术标准的要求，对公有云个人信息安全管理体系认证实施过程作出具体规定，明确EWC对认证过程的管理责任，保证公有云个人信息安全管理体系认证活动的规范有效。

1.3 本规则是EWC及受审核方与获证组织在公有云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 引用文件

下列文件对于本文件的应用是必不可少的，凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是不注日期的引用文件，其最新版本适用于本文件。

ISO/IEC 17021-1:2021 《合格评定 管理体系审核认证机构的要求》

ISO 19011:2018 《管理体系审核指南》

3 认证依据

ISO/IEC 27018：2019 《信息技术 安全技术 个人信息身份信息处理者在公有云中保护个人身份信息的实践指南》

EWC-R-TC 001:2025 《特定管理体系 要求》

4 EWC 认证管理要求

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EWC内部质量管理体系，以使从事的认证活动符合相关认证认可行业要求。

4.3 建立内部制约、监督和责任机制，实现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 对认证人员的要求

4.4.1 认证审核员应为国家注册管理体系审核员。

4.4.2 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 申请方/受审核方的义务

5.1 申请方、受审核方在认证过程中应配合EWC认证过程管理活动，协作完成认证过程各阶段的相应活动。

5.2 申请方、受审核方应履行以下职责及义务：

（1）按本中心要求提交认证申请文件及相关资料；

（2）为认证审核组提供必要的食、宿、行及办公条件，以保证审核顺利进行；

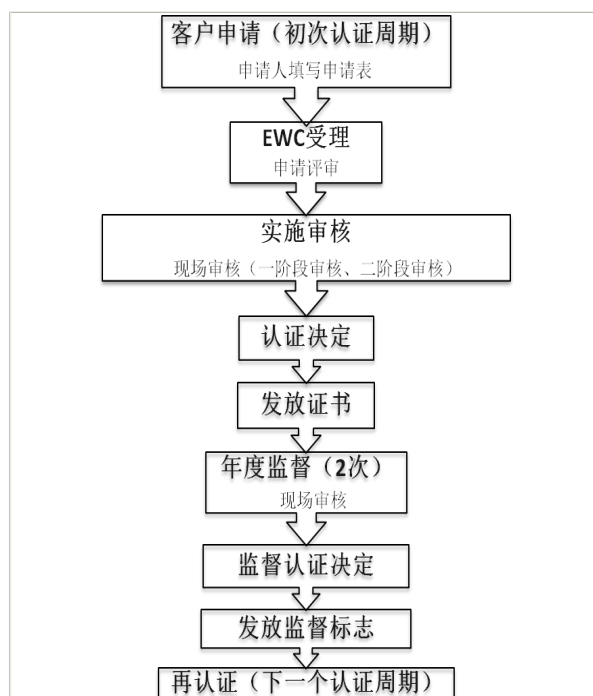
（3）为认证审核组进入审核区域、调阅文件记录、访问相关人员等提供必要的条件；适用时，为接纳到场的观察员（如认可机构评审员）提供条件。

（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及纠正措施记录，并在本中心要求时提供。重要投诉应及时通报本中心。

（5）按规定及时交纳认证费用。

6 认证实施程序

6.1 认证流程



6.2 认证申请与评审

6.2.1 申请方应符合以下条件

（1） 中国企业取得《企业法人营业执照》；外国企业持有关机构的登记注册证明。当所从事的活动有准入等资质许可要求时还应具备相应的许可资质，如：生产许可证、安全生产许可证、排污许可证等。

（2） 已按认证标准的要求建立管理体系，制定方针、目标及相应的管理文件，且体系实施运行 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） 未列入国家信用信息严重失信主体名录。

6.2.2 申请组织应向EWC提交以下资料：

（1） 认证申请书。

（2） 企业法律地位证明文件（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。若申请认证的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) 申请认证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) 申请人已按认证标准建立并实施的相关文件，如：手册、程序等。

6.2.3 EWC 应对认证申请及补充信息进行评审，确保足以建立审核方案，并确保解决了EWC与申请方之间任何已知的理解差异。

6.2.4 EWC 应根据申请方所申请的认证范围、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（语言、安全条件、对公正性的威胁等），综合确定是否有能力受理认证申请。

6.2.5 经评审符合要求的，EWC可决定受理认证申请；对不符合要求的，EWC应记录拒绝申请的原因并将该原因通知申请方。

6.2.6 EWC 应完整保存认证申请的评审工作记录。

6.2.7 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获证体系的承诺。

(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企业发生与获证体系相关的事故。

②体系相关情况发生变更，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；认证范围所覆盖的活动范围变更；认证范围内重要过程的重大变更等。

③出现影响获证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；不得擅自利用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。

6.3 审核策划

6.3.1 审核方案

(1) 认证周期内的审核方案策划，包括两个阶段的初次审核、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) EWC根据组织的规模、体系、产品和过程范围与复杂程度、管理体系有效性及以往审核的结果，建立认证周期审核方案。

6.3.2 审核时间

为确保认证审核的完整有效，EWC根据申请方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。

6.3.3 多场所抽样

当受审核方的管理体系包括多个地址进行相同的活动时，EWC依从本中心《多场所认证管理程序》对多场所情况进行评审分析，适用时制定抽样审核方案。

6.3.4 确定审核目的、范围、准则

(1) EWC根据申请方的申请信息及本认证规则确定审核目的、审核范围及准则，包括任何更改，并在与申请方商讨后确定。

(2) 审核目的包括：确定管理体系与审核准则的符合性；确定体系具备保证满足适用的法律法规及合同要求的能力；确定管理体系能够合理预期实现其规定的目标方面的有效性；适用时，识别体系的潜在改进区域。

(3) 审核范围包括：审核的内容和界限，如审核的场所、单元、活动及过程。

(4) 审核准则包括：认证依据的标准及规范性文件；管理体系的过程和文件。

6.3.5 审核组的选择和指派

(1) EWC根据体系覆盖的活动选择具备相关能力的审核员和（或）技术专家组成审核组。适用时，审核组内还包括观察员。审核组中的审核员应承担审核责任。

(2) 技术专家主要负责提供认证审核的技术支持，不作为审核员单独开展审核，其工作时间不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

(3) 实习审核员应在审核员的指导下参与审核，其工作时间不计入审核时间，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。

6.3.6 审核计划

(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/场所、审核时间、审核组成员及同行人员的角色和职责。

(2) 如果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 依从本中心《多场所认证管理程序》对多场所情况进行评审分析，并最终决定是否在审核中执行抽样审核。

(3) 现场审核前，审核组应将审核计划提交EWC及受审核方确认。遇特殊情况临时变更计划时，应及时将变更情况告知EWC及受审核方，并经三方协商一致。

6.4 初次审核

6.4.1 初次认证审核分为第一、二阶段审核。

6.4.2 审核组应当按照审核计划的安排召开首次会议、进行各场所/部门/过程审核、开展审核中的沟通、召开末次会议等已策划的工作。审核计划的修改应经受审核方及EWC共同确认后方可实施。

6.4.3 第一阶段审核

6.4.3.1 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申请认证的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申请认证的认证标准要求的情况，评价申请认证的管理体系运行过程中是否实施了内部审核与管理评审。对申请认证的管理体系文件化信息不符合现场实际，以及其他不具备第二阶段审核条件的，应当不实施第二阶段审核。

(3) 确认受审核方建立的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) 结合管理体系覆盖产品和服务的特点识别对体系管理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。

6.4.3.2 在下列情况, 第一阶段审核可以不在受审核方现场进行:

(1) 受审核方已获 EWC 颁发的其他有效认证证书, EWC 已对受审核方有充分了解。

(2) 受审核方获得了其他经认可的认证机构颁发的所申请认证管理体系有效状态的认证证书, 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。

6.4.3.3 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。

6.4.4 第二阶段审核

6.4.4.1 第二阶段审核重点是审核受审核方申请认证的管理体系符合认证标准要求 and 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) 为实现管理体系方针而在相关职能、层次和过程上建立的管理目标是否具体适用、可测量并得到沟通、监视。

(3) 对申请认证的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。

6.4.4.2 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) 受审核方的管理体系有重大缺陷, 不符合认证标准的要求。

(3) 发现受审核方存在重大问题或有其他与申请认证的管理体系相关的严重违法违规行为。

(4) 其他导致审核程序无法完成的情况。

6.5 审核报告

6.5.1 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。

（4）审核活动的实施日期和地点，适用时还包括偏离审核计划的情况说明、对审核风险及影响审核结论的不确定性的客观陈述。

（5）审核工作情况，包括审核计划安排、审核证据、审核发现和审核结论；对管理体系目标、过程及体系绩效实现情况进行评价。

（6）识别出的不符合项。

（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。

6.5.2 EWC应保留用于证实审核报告中相关信息的证据。

6.5.3 EWC应在作出认证决定后30个工作日内将审核报告提交认证申请方。

6.5.4 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认证申请方。

6.6 不符合项的纠正和纠正措施及其结果的验证

6.6.1 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。当审核期间发现组织存在严重不符合，审核组长现场与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，最长不超过6个月。如果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。

6.6.2 EWC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。

6.7 认证决定

6.7.1 EWC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的基础上，作出认证决定并保持认证决定记录。

6.7.2 EWC在作出认证决定前应确认如下情形：

（1）审核报告符合要求，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在持续改进管理体系的有效性方面存在缺陷，实现管理目标有重大疑问。

②制定的管理目标不可测量、或测量方法不明确。

③对实现管理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。

6.7.3 EWC经评定证明受审核方满足以下要求的，向其颁发认证证书。

（1）受审核方申请认证的管理体系符合认证依据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。

6.7.4 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，EWC应及时告知受审核方并说明其未通过认证的原因。

6.7.5 EWC 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认证机构上报的认证证书等信息。

6.8 监督审核程序

6.8.1 EWC对持有EWC颁发的本管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织所获认证的管理体系的持续符合性。

6.8.2 EWC将根据获证组织的管理体系认证范围内活动的风险程度或其他特性，

确定对获证组织的监督审核的频次。

6.8.3 作为最低要求，获证组织在认证周期内至少需接受两次监督审核，两次监督审核的时间间隔不得超过15个月。

6.8.4 获证组织在认证周期内超过期限而未能进行监督审核的，EWC将对其认证证书予以暂停，暂停期满仍未能接受审核的将对认证证书予以撤销。

6.8.5 监督审核的时间应为初评审核时间的三分之一。

6.8.6 监督审核时至少应审核以下内容：

（1）上次审核已获证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）重要关键点是否按获证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）获证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）管理体系目标及管理体系绩效信息。当目标及绩效没有实现时，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，是否及时制定并实施了有效的改进措施。

6.8.7 监督审核的审核报告应描述审核证据、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。

6.8.8 EWC 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。

6.9 再认证程序

6.9.1 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。

6.9.2 再认证的申请及评审、审核策划、认证过程同初次认证。

6.9.3 在获证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。当管理体系、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。

6.9.4 再认证审核时间应不少于初次认证审核的 2/3。

6.9.5 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。

6.9.6 EWC 再认证决定过程同初次认证。确认获证组织继续满足认证要求并履行认证合同义务的，EWC 将向其换发认证证书。

6.9.7 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，则不予以再认证，也不延长认证的效力。

6.9.8 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。

7 认证证书状态管理

7.1 EWC 依据《认证暂停、撤销、缩小管理程序》对获认证组织的认证证书进行管理。

7.2 暂停证书

7.2.1 获证组织有以下情形之一的，EWC 应在调查核实后暂停其认证证书。

（1）获证管理体系持续或严重不满足认证要求，包括体系运行有效性不满足要求。

（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。

7.2.2 认证证书暂停期一般不超过 6 个月。但属于 7.2.1 第（5）项情形的暂停期可至相关单位作出许可决定之日。

7.2.3 获证组织在接到 EWC 暂停通知后，在暂停期间不得以任何方式使用认证证书、认证标识或引用认证信息。

7.3 撤销证书

7.3.1 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）有其他严重违法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）没有运行获证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。

7.3.2 撤销认证证书后，EWC 将通知获证组织向 EWC 返还认证证书。

7.4 暂停及撤销信息的公示

EWC 暂停或撤销认证证书后，将在 EWC 网站上对暂停及撤销信息予以公布，同时按规定程序和要求报国家认监委，以采取措施避免各类无效的认证证书和认证标志被继续使用。

8 认证证书要求

8.1 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) 管理体系覆盖的生产经营或服务的地址和业务范围。若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) 管理体系符合认证标准的表述，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) 证书有效期的起止年月日。

证书将注明 “证书的有效性需经 EWC 通过定期的监督审核确认保持” 的提示信息。

(7) 证书查询方式。EWC 认证证书除可在本机构网站上的查询方式外，还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。

8.2 初次认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 年。

8.3 EWC 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，还将根据社会相关方的请求向其提供认证证书信息，接受社会监督。

9 与其他管理体系的结合审核

9.1 当所认证的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各体系的要求，并易于识别。

9.2 结合审核的审核时间不得少于多个单独体系所需审核时间之和的 80%。

10 组织的申诉及投诉

10.1 受审核方或获证组织对审核组或 EWC 的认证决定有异议时，可向 EWC 提出申诉或投诉。

10.2 EWC 依据《投诉、申诉和争议处理程序》，选择与申诉及投诉无关的管理人员负责开展对申诉及投诉的调查及作出处理决议，并在 60 日内将处理结果形成书面通知送交申诉人。

10.3 申诉/投诉人若认为 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继续投诉。

11 认证记录的管理

11.1 EWC 建立《记录管理程序》，对认证活动过程建立并保持记录，并妥善保存。

11.2 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。

12 其他

12.1 本规则内容提及认证标准时均指认证活动发生时认证标准的有效版本。认证活动及认证证书中描述认证标准号时，应采用当时有效版本的完整标准号。

12.2 EWC 对受审核方可开展管理体系及相关技术标准的宣贯，促使组织的全体员工正确理解和执行管理体系标准。

附录 A（规范性附录）

审 核 时 间

公有云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，并且范围覆盖了公有云个人信息安全管理体认证申请范围，则公有云个人信息安全管理体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，则公有云个人信息安全管理体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）。

公有云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）。