中鸿认证（江苏）有限公司其他管理体系审核标准

公有云个人可识别信息保护管理体系认证技术规范

2025-07-18发布 2025-07-18实施

中鸿认证（江苏）有限公司发布

前言

本文件按照GB/T1.1-2020《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。

本文件由中鸿认证（江苏）有限公司技术部提出并归口。

本文件起草单位：中鸿认证（江苏）有限公司

本文件主要起草人：孙敬、韩自鹤、丁泽林

引言

随着云计算成为全球数字经济的核心基础设施，公有云服务提供商在提供弹性、可扩展计算资源的同时，亦承担着代表云服务客户处理海量个人可识别信息（PII）的角色。不同司法管辖区对PII保护的法律、监管要求差异显著，导致跨国运营面临合规碎片化风险。本标准为公有云服务商提供一套强制性的管理体系框架，确保其作为PII处理者时满足相关标准法规要求及各区域数据保护法规的统一落地。

本标准规定公有云服务商作为PII处理者时，建立、实施并保持个人可识别信息保护管理体系的强制性要求，旨在确保PII全生命周期安全，支撑云服务客户与监管机构的信任。

本标准适用于任何规模、类型和地域的公有云组织，涵盖各种服务形态；不适用于服务商自身作为PII控制者的场景。

公有云中个人可识别信息保护管理体系要求

1.范围

本标准规定了公有云服务商作为个人可识别信息（PII）处理者时，公有云中个人可识别信息保护管理体系的建立、实施、保持和持续改进的要求，为公有云计算环境下，组织实施保护PII的控制提供了通用的控制目标、控制措施和指南。

本标准适用于任何规模、类型和性质的提供公有云服务的组织。这些组织作为PII处理者与其他组织签订合同，提供云计算环境下的信息处理服务。

2.规范性引用文件

下列文件对于本标准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标准。凡是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。

(1) ISO/IEC27001信息安全网络安全与隐私保护—信息安全管理体系要求

(2) ISO/IEC27018信息技术—安全技术—公有云环境下作为PII处理者保护个人可识别信息（PII）的实践指南

(3) ISO/IEC29100信息技术—安全技术—隐私框架

(4) ISO9001质量管理体系要求

3.术语和定义

基于本标准的目的，ISO/IEC27001以及下列术语和定义适用于本文件。

3.1个人可识别信息PersonallyIdentifiableInformation(PII)

任何可用于与相关自然人建立关联关系的信息；或能够直接或间接地关联到自然人的信息。

注：定义中的“自然人”是PII主体（3.3）。为了确定PII主体是否可识别，应考虑持有数据的隐私利益相关方或任何其他方可以合理使用的所有方法，以建立在PII集和自然人之间的联系。

3.2 PII控制者PIIController

决定个人身份信息（PII）（3.1）处理目的和方法的隐私利益相关者（或多个隐私利益相关者），因个人目的使用数据的自然人除外。

注：PII控制者有时会指示其他人（例如，PII处理者（3.4）]代表其处理PII，而处理责任仍由PII控制者承担。

3.3 PII主体PIIPrincipal

个人可识别信息（PII）（3.1）所标识的或关联的自然人。

注：根据司法管辖权以及特定的PII保护和隐私立法，也可以使用同义词“数据主体”代替术语“PII主体”。

3.4 PII处理者PIIprocessor

代表处理个人可识别信息（PII）控制者并按照其指示处理个人可识别信息的隐私利益相关方（3.2）。

3.5 公有云服务提供商publiccloudserviceprovider

根据公有云模型提供云服务的一方。

4.组织环境

4.1理解组织及其环境

组织应确定与其PII保护目的相关并影响实现管理体系预期结果能力的外部和内部因素，包括：

a）适用的数据保护法律、监管要求；

b）云服务客户合同要求；

c）市场、供应链、技术、安全威胁变化。

4.2理解相关方需求

组织应识别：

a）云服务客户、PII主体、监管机构、分包商；

b）上述各方关于PII保护的强制性要求；

组织应持续监视和评审这些相关方及其要求的相关信息。

4.3确定公有云中个人可识别信息保护管理体系的范围

组织应确定公有云中个人可识别信息保护管理体系的范围，该范围应界定公有云中个人可识别信息保护管理体系的边界和适用性，包括：

a）处理的PII类型、类别；

b）服务交付模型；

c）地理区域、数据中心、分包商。

确定范围时，组织应考虑：

a）4.1中提到的内部和外部因素；

b）4.2中提到的相关方的要求。

5.领导作用

5.1领导作用和承诺

最高管理者应通过以下方面，证实其对公有云中个人可识别信息保护管理体系的领导作用和承诺：

a）对公有云中个人可识别信息保护管理体系的有效性负责；

b）确保制定公有云中个人可识别信息保护管理体系方针和公有云中个人可识别信息保护管理体系目标，并确保其与组织战略方向一致；

c）确保公有云中个人可识别信息保护管理体系融入组织的业务过程；

d）促进使用过程方法和基于风险的思维；

e）确保获得公有云中个人可识别信息保护管理体系所需的资源；

f）沟通有效的公有云中个人可识别信息保护管理及符合公有云中个人可识别信息保护管理体系要求的重要性；

g）确保公有云中个人可识别信息保护管理体系实现其预期结果；

h）指导并支持员工为公有云中个人可识别信息保护管理体系的有效性做出贡献；

i）促进持续改进；

j）支持其他相关管理者在其职责范围内发挥领导作用。

5.2公有云中个人可识别信息保护管理体系方针

最高管理者应在考虑相关方需求和期望的基础上制定公有云中个人可识别信息保护管理体系方针，方针应：

a）适应组织的宗旨和环境；

b）为制定公有云中个人可识别信息保护管理体系目标提供框架；

c）包括满足适用要求的承诺；

d）包括持续改进公有云中个人可识别信息保护管理体系的承诺；

e）由最高管理者制定并批准；

f）在组织内得到沟通和理解；

g）形成文件化信息并可为相关方所获取。

5.3组织的岗位、职责和权限

最高管理者应确保组织内相关岗位的职责和权限得到分配、沟通和理解。公有云中个人可识别信息保护管理体系的职责和权限应予以明确，形成文件化信息并在组织内沟通，以确保公有云中个人可识别信息保护管理体系的有效运行。

6.策划

6.1应对风险和机遇的措施

6.1.1总则

组织应策划：

a）在确定需要应对的风险和机遇以及如何应对时，应考虑：

1）公有云中个人可识别信息保护管理体系的范围；

2）公有云中个人可识别信息保护管理体系方针；

3）公有云中个人可识别信息保护管理体系目标及其为实现这些目标所策划的措施；

4）适用的法律法规要求和组织应遵守的其他要求；

5）相关方的要求；

6）组织的内部和外部环境。

b）应对风险和机遇的措施应与风险和机遇对公有云中个人可识别信息保护管理体系预期结果的潜在影响相适应，并包括：

1）规避风险；

2）接受风险以利用机遇；

3）消除风险源；

4）改变风险的可能性或后果；

5）分担风险；

6）基于信息做出决策；

7）评估所采取措施的有效性；

8）将风险控制在可接受水平。

6.1.2公有云中个人可识别信息保护风险评估与处置

组织应建立、实施和维护一个PII安全风险评估过程，以识别和评估与PII相关的安全风险。风险评估应包括：

a）建立并维护信息安全风险准则，包括：

1）风险接受准则；

2)PII安全风险评估实施准则。

b）识别PII生命周期内所有处理活动；

c）评估每项活动对PII主体的风险；

d）识别法律、合同、声誉风险；

e）确定风险等级，并制定相应的风险处置措施。

风险处置措施应包括：

a）在考虑风险评估结果的基础上，选择适合的PII安全风险处置选项；

b）确定实现已选的PII安全风险处置选项所必需的所有控制；注1：当需要时，组织可设计控制，或识别来自任何来源的控制。

c）制定一个适用性声明，包含：

—必要的控制；

—及其选择的合理性说明；

—该控制是否已实现；

d）制定正式的PII安全风险处置计划；

e）获得风险责任人对PII安全风险处置计划以及对PII安全残余风险的接受的批准。

组织应保留有关PII安全风险评估过程的文件化信息

6.2公有云中个人可识别信息保护管理体系目标及其实现的策划

组织应制定公有云中个人可识别信息保护管理体系目标，并策划实现这些目标所需的措施。

公有云中个人可识别信息保护管理体系目标应：

a）与公有云中个人可识别信息保护管理体系方针保持一致；

b）可测量（可行时）；

c）考虑适用的要求；

d）与组织在PII安全方面的风险和机遇相关；

e）得到监视；

f）得到沟通；

g）适时更新。

组织应保留有关公有云中个人可识别信息保护管理体系目标的文件化信息。

策划措施时，组织应考虑：

a）需要做什么；

b）需要什么资源；

c）谁负责；

d）何时完成；

e）如何评价结果。

6.3变更规划

当组织确定需要对公有云中个人可识别信息保护管理体系进行变更时，应以策划的方式进行变更。

7.支持

7.1资源

组织应确定并提供所需的资源，以建立、实施、保持和持续改进公有云中个人可识别信息保护管理体系。

资源包括：

a）人力资源；

b）技术资源；

c）财务资源；

d）信息资源；

e）基础设施资源。

7.2能力

组织应：

a）确定在其控制下工作，对公有云中个人可识别信息保护管理体系绩效和有效性有影响的人员所需具备的能力；

b）基于适当的教育、培训或经验，确保这些人员是胜任的；

c）适用时，采取措施以获得所需的能力，并评价所采取措施的有效性；

d）保留适当的成文信息，作为人员能力的证据。

7.3意识

组织应确保在其控制下工作的人员意识到：

a）公有云中个人可识别信息保护管理体系方针；

b）公有云中个人可识别信息保护管理体系相关要求；

c）他们对公有云中个人可识别信息保护管理体系有效性的贡献，包括改进公有云中个人可识别信息保护管理体系绩效的益处；

d）不符合公有云中个人可识别信息保护管理体系要求的后果。

7.4沟通

组织应确定与公有云中个人可识别信息保护管理体系相关的内部和外部沟通，包括：

a）沟通内容；

b）何时沟通；

c）与谁沟通；

d）如何沟通；

e）谁负责沟通。

7.5文件化信息

7.5.1总则

公有云中个人可识别信息保护管理体系成文信息应包括：

a）本标准要求的成文信息；

b）组织确定的为确保公有云中个人可识别信息保护管理体系有效性所需的成文信息。

7.5.2创建和更新

在创建和更新成文信息时，组织应确保适当的：

a）标识和说明（如标题、日期、作者）；

b）形式和载体（如纸质、电子）；

c）评审和批准，以保持适宜性和充分性。

7.5.3文件化信息的控制

组织应控制公有云中个人可识别信息保护管理体系和相关成文信息，以确保：

a）在需要的场合和时间，均可获得并适用；

b）得到充分保护（如防止失密、不当使用或完整性受损）。

为控制成文信息，适用时，组织应进行下列活动：

a）分发、访问、检索和使用；

b）存储和保护，包括保持可读性；

c）变更的控制（如版本控制）；

d）保留和处置。

8.运行

8.1运行的策划和控制

组织应策划、实施和控制满足公有云中个人可识别信息保护管理体系要求和实施第6章所确定的措施所需的过程，通过：

a）建立过程准则；

b）按照准则实施过程；

c）保持所需的成文信息，以确信过程已按策划进行；

d）实施变更以实现改进结果；

e）确保可获得过程所需的资源；

f）分配过程的职责和权限；

g）监视和评审过程的实施情况，以确保其有效性。

8.2与客户的合同要求

与公有云服务客户的合同或正式协议应包括：

a）处理目的、类别、期限；

b）云服务客户与组织间责任分配矩阵；

c）PII主体权利实现机制；

d）分包商使用与变更通知条款；

e）数据泄露通知时限（不晚于72小时）；

f）数据返还、转移、删除方式；

g）审计权利与方式。

8.3PII处理控制措施

组织应确保：

a）仅依云服务客户指令处理PII；

b）不将PII用于营销或广告；

c）采用加密、匿名化、访问控制等技术；

d）记录处理活动日志，保存不少于12个月；

e）按生命周期阶段执行最小化、限制披露、及时删除。

8.4分包处理

组织应：

a）通过合同、协议等方式要求分包商遵守本标准要求；

b）建立分包商PII处理清单并动态更新；

c）将分包商变更提前30日书面通知云服务客户。

9绩效评价

9.1监视、测量、分析和评价

9.1.1总则

组织应建立、实施和维护一个监视、测量、分析和评价公有云中个人可识别信息保护管理体系绩效的过程。该过程应确保：

a）公有云中个人可识别信息保护管理体系的有效性；

b）满足相关方的要求；

c）实现公有云中个人可识别信息保护管理体系目标；

d）持续改进公有云中个人可识别信息保护管理体系的适宜性、充分性和有效性。

9.1.2顾客满意

组织应监视顾客对其需求和期望得到满足的感知程度。组织应确定这些感知的信息来源、监视方法和频次。组织应保留有关顾客满意信息的成文信息。

9.1.3分析与评价

组织应分析和评价通过监视和测量获得的适当数据和信息。分析和评价应利用适宜的方法，以确保公有云中个人可识别信息保护管理体系的有效性，并为持续改进提供依据。分析和评价的结果应用于：

a）评估公有云中个人可识别信息保护管理体系的绩效和有效性；

b）确定公有云中个人可识别信息保护管理体系的改进机会；

c）评估风险和机遇的应对措施的有效性；

d）支持决策，以实现公有云中个人可识别信息保护管理体系的持续改进。

9.2内部审核

9.2.1总则

组织应按照策划的时间间隔进行内部审核，以确定公有云中个人可识别信息保护管理体系是否：

a）符合组织自身的要求；

b）符合本标准的要求；

c）得到有效实施和保持。

9.2.2审核方案

组织应：

a）策划、制定、实施和维护一个或多个审核方案，考虑有关过程的重要性、对组织产生影响的变化以及以往审核的结果；

b）规定每次审核的审核准则、范围、频次和方法。

内部审核应由与被审核活动无直接责任的人员实施，除非组织规模较小或审核范围有限，可由其他胜任的人员实施。

9.2.3审核实施

组织应确保：

a）审核员的独立性和客观性；

b）审核过程的透明性和公正性；

c）审核结果的准确性和可靠性。

审核结果应形成文件，并提交给相关管理者进行评审。

9.2.4审核结果

组织应：

a）对内部审核的结果进行评审，以确定公有云中个人可识别信息保护管理体系的有效性；

b）对内部审核中发现的不符合项采取纠正措施；

c）对内部审核中发现的改进机会采取措施；

d）保留内部审核的成文信息，作为审核实施和结果的证据。

9.3管理评审

9.3.1总则

最高管理者应按照策划的时间间隔对组织的公有云中个人可识别信息保护管理体系进行评审，以确保其持续的适宜性、充分性和有效性。管理评审应包括对公有云中个人可识别信息保护管理体系改进机会和变更需求的评价。

9.3.2管理评审输入

管理评审的输入应包括：

a）以往管理评审的跟踪措施；

b）与公有云中个人可识别信息保护管理体系相关的内外部因素的变化；

c）顾客反馈和相关方的反馈；

d）公有云中个人可识别信息保护管理体系绩效的监视和测量结果；

e）审核结果；

f）风险和机遇的应对措施的有效性；

g）不符合项和纠正措施的状态；

h）公有云中个人可识别信息保护管理体系目标的完成情况；

i）资源的适宜性；

j）持续改进的机会。

9.3.3管理评审输出

管理评审的输出应包括与以下方面相关的决策和措施：

a）公有云中个人可识别信息保护管理体系的改进；

b）产品和服务的改进；

c）资源的需求；

d）变更的需求。

管理评审的结果应形成文件，并在组织内进行沟通。

10改进

10.1总则

组织应通过以下方面持续改进公有云中个人可识别信息保护管理体系的适宜性、充分性和有效性：

a）分析和评价监视和测量的结果；

b）实施内部审核和管理评审的结果；

c）采取纠正措施和预防措施；

d）更新风险和机遇的应对措施；

e）改进公有云中个人可识别信息保护管理体系的过程和控制措施。

10.2不符合和纠正措施

10.2.1总则

组织应采取措施，以消除不符合的原因，防止不符合再次发生或在其他地方发生。纠正措施应与所发生的不符合的影响相适应。

10.2.2纠正措施的要求

组织应：

a）对不符合进行评审；

b）确定不符合的原因；

c）确定是否存在或可能发生类似的不符合；

d）实施必要的纠正措施；

e）对采取的纠正措施进行评审，以确保其有效性；

f）保留不符合的性质以及随后所采取的措施的成文信息。

10.3持续改进

组织应持续改进公有云中个人可识别信息保护管理体系的适宜性、充分性和有效性。持续改进应包括：

a）对公有云中个人可识别信息保护管理体系进行评审和分析；

b）识别改进机会；

c）实施改进措施；

d）评估改进措施的效果；

e）更新公有云中个人可识别信息保护管理体系的目标和控制措施；

f）确保改进措施与组织的战略方向一致。

通过持续改进，组织应能够更好地改进公有云中个人可识别信息保护管理体系的适宜性，提高公有云中个人可识别信息保护管理体系的有效性，满足相关方的要求，并实现公有云中个人可识别信息保护管理体系的持续改进。