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。

中鸿认证（江苏）有限公司其他管理体系审核标准

数据安全能力成熟度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

以数据安全为关注焦点是组织数据管理的重要原则。本标准采用过程方法，结合PDCA（策划 - 实施 - 检查 - 改进）循环和基于风险的思维，旨在帮助组织在不断变化的环境中实现持续改进。

本标准规定了组织建立、实施、维护和持续改进数据安全能力成熟度管理体系的要求。本标准适用于组织对数据安全管理的全过程控制，旨在通过规范的管理体系，提升组织的数据安全能力。

数据安全能力成熟度管理体系要求

1.范围

本标准规定了组织建立、实施、保持并持续改进数据安全能力成熟度管理体系（以下简称DSMMS）的通用要求，适用于任何类型、规模和性质的组织，可作为内部审核或第三方认证的依据。

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/T37988—2019信息安全技术数据安全能力成熟度模型

3.术语和定义

3.1数据安全能力成熟度模型DSMM

按照GB/T37988-2019第3.7条定义。

3.2数据安全能力成熟度管理体系DSMMS

组织依据本标准，围绕数据生命周期安全能力，对“组织建设、制度流程、技术工具、人员能力”四维进行策划、实施、评价和改进的管理体系。

3.3缩略语

GB/T37988-2019第4章使用的下列缩略语用于本文件。

BP：基本实践（Base Practice）

PA：过程域（Process Area）

4.组织环境

4.1理解组织及其环境

组织应识别影响数据安全能力成熟度的内外部因素并形成文件。

4.2理解相关方的需求和期望

组织应确定：

a）与数据安全能力成熟度管理体系相关的利益相关方；

b）这些利益相关方的要求；

c）组织应监视和评审这些利益相关方的信息及其相关要求。

4.3确定数据安全能力成熟度管理体系的范围

组织应确定数据安全能力成熟度管理体系的边界及其适用性，以确定其范围。

在确定范围时，组织应考虑：

a）4.1中提到的外部和内部因素；

b）4.2中提到的要求。

4.4数据安全能力成熟度管理体系

组织应按照本文件的要求，建立、实现、维护和持续改进数据安全能力成熟度管理体系，包括所需的过程及其相互作用。

5领导作用

5.1领导和承诺

最高管理者应通过以下方面，证实其对数据安全能力成熟度管理体系的领导作用和承诺：

a）确保建立了数据安全能力成熟度管理体系方针，并与组织环境相适应，与战略方向相一致；

b）确保将数据安全能力成熟度管理体系要求融入组织的业务过程；

c）确保数据安全能力成熟度管理体系所需资源可用；

d）沟通有效的数据安全能力成熟度管理和数据安全能力成熟度管理体系要求的重要性；

e）指导并支持相关人员为数据安全能力成熟度管理体系的有效性做出贡献；

f）确保数据安全能力成熟度管理体系实现其预期结果；

g）促进持续改进；

h）支持其他相关管理角色，以证实他们的领导角色应用于其责任范围。

5.2方针

最高管理者应建立数据安全能力成熟度管理体系方针，该方针应：

a）与组织意图相适宜；

b）为建立数据安全能力成熟度目标提供框架；

c）包括满足适用要求的承诺；

d）包括持续改进数据安全能力成熟度管理体系的承诺。

建立数据安全能力成熟度方针应：

a）形成文件化信息并可用；

b）在组织内得到沟通；

c）适当时，对相关方可用。

5.3组织的角色、职责和权限

最高管理者应确保相关角色的职责和权限在组织内得到分配和沟通。

最高管理者应在以下方面分配职责和权限：

a）确保数据安全能力成熟度管理体系符合本文件的要求；

a）向最高管理者报告数据安全能力成熟度管理体系的绩效。

6策划

6.1应对风险和机遇的措施

总则当规划数据安全能力成熟度管理体系时，组织应考虑4.1所提及的事项和4.2所提及的要求，并确定需要应对的风险和机遇，以便：

a）确保数据安全能力成熟度管理体系达到预期结果；

b）预防或减少不良影响；

c）实现持续改进。

组织应策划：

d）应对这些风险和机遇的措施；

e）如何

1）将这些措施整合到数据安全能力成熟度管理体系过程中，并予以实现；

2）评价这些措施的有效性。

6.2数据安全目标及其实现的策划

将GB/T37988-2019文件5.3中的数据安全能力成熟度等级1-5级中的相应等级作为组织的总体目标，并依据GB/T37988-2019文件5.4.2中的数据安全PA体系，将目标分解为可测量、可追踪的子目标，明确资源、时间表及责任人。

6.3变更的策划

当组织确定需要对数据安全能力成熟度管理体系进行变更时，变更应按所策划的方式实施。

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、维护和持续改进数据安全能力成熟度管理体系。

7.2能力

从组织内承担数据安全工作的人员应具备的能力出发，并考虑以下方面：

a）数据安全人员所具备的数据安全技能应能够满足实现安全目标的能力要求（对数据相关业务的理解程度以及数据安全专业能力）；

b）应根据安全目标对数据安全人员的数据安全意识以及对关键数据安全岗位员工数据安全能力进行培养。

7.3意识

组织应确保在其控制下工作的人员知晓：

a）数据安全能力成熟度管理体系方针；

b）其对数据安全能力成熟度管理体系有效性的贡献，包括改进绩效的益处；

c）不符合数据安全能力成熟度管理体系要求的后果。

7.4沟通

组织应确定与数据安全能力成熟度管理体系相关的内部和外部沟通，包括：

a）沟通什么；

b）何时沟通；

c）与谁沟通；

d）如何沟通；

e）由谁沟通。

7.5文件化信息

7.5.1总则

组织的数据安全能力成熟度管理体系应包括：

a）本文件要求的文件化信息；

b）本文件所确定的、为确保数据安全能力成熟度管理体系有效性所需的文件化信息。注：

对于不同组织，数据安全能力成熟度管理体系文件化信息的多少与详略程度可以不同，取决于：

1）组织的规模及其活动、过程、产品和服务的类型；

2）过程及其相互作用的复杂程度；

3）人员的能力。

7.5.2创建和更新

在创建和更新文件化信息时，组织应确保适当的：

a）标识和说明（如标题、日期、版本、作者或引用编号）；

b）形式（如语言、软件版本、图表）和载体（如纸质的、电子的）；

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

应控制数据安全能力成熟度管理体系和本文件所要求的文件化信息，以确保：

a）在需要的场合和时机，均可获得并适用；

b）予以妥善保护（如防止泄密、不当使用或缺失）。

为控制文件化信息，适用时，组织应进行以下活动：

a）分发、访问、保密级别、检索和使用；

b）存储和防护，包括保持可读性；

c）变更控制（如版本控制）；

d）保留和处置。

对于组织确定的策划和运行数据安全能力成熟度管理体系所必需的来自外部的文件化信息，组织应进行适当识别，并予以控制。

注：对文件化信息的“访问”可能意味着仅允许查阅，或者意味着允许查阅并授权修改。

8运行

8.1运行的策划和控制

组织应按GB/T37988-2019的数据安全能力成熟度模型，结合自身的数据安全目标，将30个过程域（PA01-PA30）的要求转化为运行准则并实施。

8.2数据安全能力等级自评估

组织应按GB/T37988-2019附录A的量化指标，结合自身的数据安全目标，使用GB/T37988-2019附录B提供的方法，按计划的时间间隔，或当重大变更提出或发生时，对自身的数据安全能力进行等级自评估，并形成自评估文件。

9绩效评价

9.1监视、测量、分析和评价

组织应确定：

a）需要监视和测量的内容；

b）适用的监视、测量、分析和评价的方法，以确保结果有效。所选的方法宜产生可比较和可再现的有效结果；

c）何时实施监视和测量；

d）谁应监视和测量；

e）何时对监视和测量的结果进行分析和评价；

f）谁应分析和评价这些结果。

组织应保留适当的文件化信息，以作为结果的证据。

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，以提供有关数据安全能力成熟度管理体系的下列信息：

a）是否符合：

1）组织自身的数据安全能力成熟度管理体系的要求；

2）本文件的要求；

b）是否得到有效地实施和保持。

9.2.2内部审核

组织应规划、建立、实现和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。

当建立内部审核方案时，应考虑相关过程的重要性和以往审核的结果。

组织应：

a）定义每次审核的审核准则和范围；

b）选择审核员并实施审核，确保审核过程的客观性和公正性；

c）确保将审核结果报告至相关管理层；

保留文件化信息作为审核方案和审核结果的证据。

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数据安全能力成熟度管理体系进行评审，以确保其持续的适宜性、充分性和有效性，并与组织的战略方向保持一致。

9.3.2管理评审输入

策划和实施管理评审时应考虑下列内容：

a）以往管理评审提出的措施的状态；

b）与数据安全能力成熟度管理体系相关的外部和内部事项的变化；

c）与数据安全能力成熟度管理体系相关的相关方需求和期望的变化；

d）有关数据安全绩效的反馈，包括以下方面的趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果；

4）数据安全目标完成情况；

e）相关方反馈；

f）数据安全能力等级自评估结果；

g）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下列事项相关的决定和措施：

a）改进的机会；

b）数据安全能力成熟度管理体系所需的变更；

c）资源需求。

组织应保留文件化信息，作为管理评审结果的证据。

10改进

10.1不合格及纠正措施

当出现不合格时，组织应：

a）对不合格做出应对，并在适用时：

1）采取措施以控制和纠正不合格；

2）处置后果；

b）通过下列活动，评价是否需要采取措施，以消除产生不合格的原因，避免其再次发生或者在其他场合发生：

1）评审和分析不合格；

2）确定不合格的原因；

3）确定是否存在或可能发生类似的不合格；

c）实施所需的措施；

d）评审所采取的纠正措施的有效性；

e）需要时，变更数据安全能力成熟度管理体系。

纠正措施应与不合格所产生的影响相适应。

组织应保留成文信息，作为下列事项的证据：

a）不合格的性质以及随后所采取的措施；

b）纠正措施的结果。

注：改进的例子可包括纠正、纠正措施、持续改进、突破性变革、创新和重组。

10.2持续改进

组织应持续改进数据安全能力成熟度管理体系的适宜性、充分性和有效性。

中鸿认证（江苏）有限公司其他管理体系审核标准

数据存储安全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

本标准旨在为组织提供一个全面的数据存储安全管理体系框架，帮助组织识别和管理数据存储过程中的安全风险，确保数据存储的安全性和合规性。本标准融合了国际先进的信息安全管理体系标准（如ISO/IEC27001、ISO/IEC27040）以及质量管理培训指南（GB/T19025-2023ISO10015:2019）的相关要求，确保组织在数据存储安全管理方面具备明确的指导和可操作的实践方法。

通过实施本标准，组织能够：

a）建立明确的数据存储安全方针和目标，确保数据存储安全管理与组织的整体战略相一致；

b）识别和评估数据存储安全风险，采取有效的控制措施，降低风险至可接受水平；

c）提高员工的数据存储安全意识和能力，通过系统的培训和持续地教育，确保员工能够履行其在数据存储安全管理体系中的职责；

d）建立有效的监测和审核机制，持续监控数据存储安全管理体系的绩效，及时发现并纠正不符合项；

e）实现数据存储安全管理体系的持续改进，通过定期的管理评审和改进措施，不断提升数据存储安全管理的水平。

本标准适用于所有涉及数据存储的组织，无论其规模大小、行业类型或业务性质。组织可以根据自身的具体情况，灵活应用本标准的要求，建立适合自身的数据存储安全管理体系。

数据存储安全管理体系要求

1.范围

本标准规定了数据存储安全管理体系的要求，旨在帮助组织建立、实施、维护和持续改进数据存储安全管理体系，以确保数据存储的安全性、可用性和完整性。本标准适用于所有涉及数据存储的组织，无论其规模大小、行业类型或业务性质。

2.规范性引用文件

以下文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

•ISO/IEC27000：信息技术-安全技术-信息安全管理体系-概述和词汇

•ISO/IEC27001：信息技术-安全技术-信息安全管理体系-要求

•ISO/IEC27002：信息技术-安全技术-信息安全控制实践指南

•ISO/IEC27040:2024数据存储安全

•GB/T19025-2023/ISO10015:2019质量管理培训指南

3.术语和定义

基于本标准的目的，ISO/IEC27000以及下列术语和定义适用于本文件。

3.1数据存储安全管理体系Data Storage Security Management System

组织为确保数据存储的安全性、可用性和完整性而建立的管理体系，包括组织结构、策略、计划、程序、过程和资源。

3.2数据存储安全风险Data Storage Security Risk

数据存储过程中可能面临的威胁、漏洞和影响的组合，可能导致数据泄露、损坏、丢失或不可用。

3.3数据存储安全控制Data Storage Security Control

为降低数据存储安全风险而采取的管理、技术和物理措施。

3.4培训training

为使员工获得或提高与数据存储安全相关的知识、技能和意识，以满足数据存储安全管理体系要求而进行的有计划的活动。

4.组织环境

4.1理解组织及其环境

组织应确定与其目标和战略方向相关并影响其实现数据存储安全管理体系预期结果的各种外部和内部因素。这些因素应包括但不限于：

a）法律法规要求；

b）技术环境；

c）数据存储的性质和规模；

d）组织的文化和价值观。

4.2理解相关方的需求和期望

组织应确定与数据存储安全管理体系有关的相关方，以及这些相关方的要求。相关方可能包括但不限于：

a）客户；

b）员工；

c）监管机构；

d）第三方服务提供商。

4.3确定数据存储安全管理体系的范围

组织应确定数据存储安全管理体系的范围，确保其涵盖所有与数据存储相关的活动、产品和服务。范围应明确界定，并形成文件。

4.4数据存储安全管理体系

组织应建立、实施、维护和持续改进数据存储安全管理体系，以确保数据存储的安全性、可用性和完整性。数据存储安全管理体系应包括但不限于以下方面：

a）数据存储安全方针和目标；

b）数据存储安全策略和程序；

c）数据存储安全风险评估和管理；

d）数据存储安全控制措施的实施；

e）数据存储安全的监测、审核和改进。

5.领导作用

5.1领导作用和承诺

最高管理者应通过以下活动，对其建立、实施、维护和持续改进数据存储安全管理体系的承诺提供证据：

a）向组织传达满足数据存储安全要求的重要性；

b）制定数据存储安全方针；

c）确保数据存储安全目标的制定；

d）进行管理评审；

e）确保资源的获得。

5.2数据存储安全方针

最高管理者应制定数据存储安全方针，方针应：

a）与组织的宗旨相适应；

b）包括对满足适用的数据存储安全要求的承诺；

c）包括对持续改进数据存储安全管理体系的承诺；

d）提供制定和评审数据存储安全目标的框架；

e）在组织内得到沟通和理解；

f）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角色的职责和权限得到分配、沟通和理解。这些角色应包括但不限于：

a）数据存储安全负责人；

b）数据存储安全团队成员；

c）数据存储管理员；

d）数据所有者。

6.策划

6.1应对风险和机遇的措施

组织应策划应对风险和机会的措施，以：

a）确保数据存储安全管理体系能够实现其预期结果；

b）预防或减少不利影响；

c）实现持续改进。

6.2数据存储安全目标及其实现的策划

组织应制定数据存储安全目标，并策划实现这些目标的措施。目标应：

a）与数据存储安全方针一致；

b）可测量；

c）考虑适用的要求；

d）与组织的业务目标相适应。

7支持

7.1资源

组织应确定并提供实施、维护和持续改进数据存储安全管理体系所需的资源，包括但不限于：

a）人力资源；

b）技术资源；

c）财务资源；

d）物理资源。

7.2能力

组织应确保其员工具备必要的能力，以履行其在数据存储安全管理体系中的职责。能力可以通过培训、教育或经验获得。

7.3意识

组织应确保其员工意识到：

a）数据存储安全的重要性；

b）个人在数据存储安全管理体系中的角色和职责；

c）偏离数据存储安全方针和程序的潜在后果。

7.4沟通

组织应建立和维护数据存储安全的内部和外部沟通机制，以确保数据存储安全信息的有效传递和共享。沟通应包括但不限于：

a）数据存储安全方针和目标的沟通；

b）数据存储安全策略和程序的沟通；

c）数据存储安全风险评估和管理的沟通；

d）数据存储安全事件的沟通。

7.5文件化信息

组织应建立和维护数据存储安全管理体系所需的文件化信息，以确保其有效性和可追溯性。文件化信息应包括但不限于：

a）数据存储安全方针和目标；

b）数据存储安全策略和程序；

c）数据存储安全风险评估和管理计划；

d）数据存储安全控制措施的实施记录；

e）数据存储安全监测和审核报告。

7.6培训

组织应根据GB/T19025-2023ISO10015:2019的要求，制定和实施数据存储安全培训计划，以提高员工对数据存储安全的认识和理解。培训计划应包括但不限于：

a）确定培训需求：组织应识别员工在数据存储安全方面的知识和技能差距，确定培训需求。

b）设计培训内容：培训内容应涵盖数据存储安全方针和目标、策略和程序、风险评估和管理、控制措施、事件响应和处理等方面。

c）实施培训：组织应采用适宜的培训方法，如课堂培训、在线培训、实践操作等，确保培训的有效性。

d）评估培训效果：组织应通过考试、实际操作测试、反馈等方式，评估培训效果，确保员工具备必要的知识和技能。

e）记录培训信息：组织应记录培训计划、培训内容、培训实施情况和培训效果评估结果，以备审核和改进。

8运行

8.1运行的策划和控制

组织应策划、实施和控制满足数据存储安全要求所需的过程，包括但不限于：

a）数据存储访问控制；

b）数据存储加密；

c）数据存储备份和恢复；

d）数据存储监控和审计；

e）数据存储漏洞管理。

8.2数据存储安全风险评估和管理

组织应建立、实施和维护数据存储安全风险评估过程，以识别和评估数据存储安全风险。风险评估应包括：

a）确定数据存储资产；

b）识别数据存储面临的威胁；

c）识别数据存储的漏洞；

d）评估数据存储安全风险的可能性和影响；

e）确定数据存储安全风险的优先级。

组织应根据风险评估的结果，制定和实施数据存储安全风险管理计划，以降低数据存储安全风险至可接受水平。风险管理计划应包括：

a）风险处理措施；

b）风险接受准则；

c）风险沟通和咨询；

d）风险监控和评审。

8.3数据存储安全控制措施

组织应根据数据存储安全风险评估的结果，选择和实施适当的数据存储安全控制措施，以确保数据存储的安全性、可用性和完整性。数据存储安全控制措施应包括但不限于：

a）数据存储访问控制；

b）数据存储加密；

c）数据存储监控和审计；

d）数据存储漏洞管理；

e）数据存储安全培训和意识提升。

8.4数据存储安全事件的响应和处理

组织应建立和实施数据存储安全事件的响应和处理机制，以确保数据存储安全事件得到及时、有效地处理。响应和处理应包括：

a）数据存储安全事件的检测和报告；

b）数据存储安全事件的影响评估；

c）数据存储安全事件的应急响应；

d）数据存储安全事件的恢复和修复；

e）数据存储安全事件的后续改进。

9绩效评价

9.1监视、测量、分析和评价

组织应建立和实施数据存储安全监测机制，以确保数据存储安全管理体系的有效运行。监测应包括：

a）数据存储安全事件的检测和记录；

b）数据存储安全控制措施的有效性评估；

c）数据存储安全风险的变化监测。

组织应定期对数据存储安全管理体系的绩效进行测量、分析和评价，以验证其符合性和有效性。测量、分析和评价应包括：

a）数据存储安全方针和目标的达成情况；

b）数据存储安全策略和程序的实施情况；

c）数据存储安全控制措施的有效性；

d）数据存储安全风险评估和管理的效果。

9.2内部审核

组织应定期进行数据存储安全内部审核，以验证数据存储安全管理体系是否符合本标准的要求，并得到有效实施和维护。内部审核应：

a）依据策划的安排进行；

b）由与被审核活动无直接责任的人员进行；

c）形成审核报告，记录审核发现和结论；

d）对审核中发现的不符合项采取纠正措施，并验证其有效性。

9.3管理评审

最高管理者应按照策划的时间间隔对数据存储安全管理体系进行评审，以确保其持续的适宜性、充分性和有效性。管理评审应包括：

a）评审数据存储安全管理体系的绩效和有效性；

b）评审数据存储安全方针和目标的达成情况；

c）评审数据存储安全风险评估和管理的效果；

d）评审数据存储安全控制措施的有效性；

e）评审数据存储安全培训和意识提升的效果；

f）评审数据存储安全事件的响应和处理情况；

g）评审数据存储安全管理体系的改进机会。

10改进

10.1不符合和纠正措施

组织应采取措施，以消除数据存储安全管理体系中的不符合原因，防止不符合的再次发生。

纠正措施应：

a）与不符合的影响相适应；

b）包括对不符合的评审和分析；

c）包括制定和实施纠正措施计划；

d）包括对纠正措施的有效性进行验证

10.2持续改进

组织应持续改进数据存储安全管理体系的适宜性、充分性和有效性。持续改进应包括：

a）对数据存储安全管理体系的绩效进行监测和测量；

b）对数据存储安全管理体系的评审结果进行分析；

c）对数据存储安全管理体系的改进机会进行识别；

d）对数据存储安全管理体系的改进措施进行策划和实施。

附录A （资料性）

A.1数据存储安全管理体系文件化信息示例：

组织应建立和维护数据存储安全管理体系所需的文件化信息，以确保其有效性和可追溯性。

文件化信息应包括但不限于：

a）数据存储安全方针和目标；

b）数据存储安全策略和程序；

c）数据存储安全风险评估和管理计划；

d）数据存储安全控制措施的实施记录；

e）数据存储安全监测和审核报告；

f）数据存储安全培训计划和记录；

g）数据存储安全事件的响应和处理记录。

A.2数据存储安全培训计划示例

组织应根据GB/T19025-2023ISO10015:2019的要求，制定和实施数据存储安全培训计划，以提高员工对数据存储安全的认识和理解。培训计划应包括但不限于：

a）确定培训需求：组织应识别员工在数据存储安全方面的知识和技能差距，确定培训需求。

b）设计培训内容：培训内容应涵盖数据存储安全方针和目标、策略和程序、风险评估和管理、控制措施、事件响应和处理等方面。

c）实施培训：组织应采用适宜的培训方法，如课堂培训、在线培训、实践操作等，确保培训的有效性。

d）评估培训效果：组织应通过考试、实际操作测试、反馈等方式，评估培训效果，确保员工具备必要的知识和技能。

e）记录培训信息：组织应记录培训计划、培训内容、培训实施情况和培训效果评估结果，以备审核和改进。

附录B（资料性）

B.1数据存储安全管理体系审核指南

组织应定期进行数据存储安全内部审核，以验证数据存储安全管理体系是否符合本标准的要求，并得到有效实施和维护。审核指南应包括但不限于：

a）审核计划的制定；

b）审核团队的组建；

c）审核实施的步骤；

d）审核报告的编写；

e）不符合项的纠正措施跟踪。

中鸿认证（江苏）有限公司其他管理体系审核标准

数据治理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

本标准规定数据治理管理体系要求，适用于组织内由IT系统创建、收集、存储、控制的数据当前及未来使用的治理，覆盖数据生命周期Collect、Store、Report、Decide、Distribute、Dispose六环节，确保数据价值实现、风险受控、约束满足。

数据治理管理体系要求

1.范围

本文件规定了组织建立、实施、保持和改进数据治理管理体系的要求。

本标准规定数据治理管理体系要求，适用于所有组织，包括公共和私营公司、政府实体和非营利组织。

本标准适用于从最小到最大的各种规模的组织，无论它们对数据的依赖程度如何。

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。

ISO/IEC38505-1:2017信息技术IT规制数据治理第1部分：ISO/IEC38500数据治理应用

3.术语和定义

ISO/IEC38500界定的以及下列术语和定义适用于本文件。

3.1 匿名化anonymization

以不可逆的方式更改个人身份信息（PII）的过程，以便PII主体不再由PII控制器单独或与任何其他方协作，无法直接或间接识别。

3.2 大数据big data

在特定问题领域的特定时间点，其特征（如数量、速度、多样性、可变性、真实性等）无法使用当前/现有/已建立/传统的技术和方法高效处理以提取价值的数据集。

注1：“大数据”（BigData）一词的使用方式多种多样，例如，它可指代用于处理海量数据集的可扩展技术。

3.3 云计算cloud computing

一种能够通过网络访问可扩展且弹性的共享物理或虚拟资源池的模式，这些资源可按需进行自助配置和管理。注1：资源示例包括服务器、操作系统、网络、软件、应用程序和存储设备。

3.4 数据问责制data accountability

对数据及其使用的问责。

注1：数据的“使用”包括与数据相关的所有活动。

3.5 去标识化de-identification

去除一组识别数据与数据主体之间关联的任何过程的通用术语。

3.6 物联网internet of things，IoT

为信息社会提供的全球基础设施，通过基于现有和不断发展的可互操作信息和通信技术，实现（物理和虚拟）事物的互联，从而提供先进服务。

注1：通过利用识别、数据捕获、处理和通信能力，物联网充分利用实物为各类应用提供服务，同时确保满足安全和隐私要求。

注2：从广义上看，物联网可被视为具有技术和社会影响的愿景。

3.7 机器学习machine learning

使用算法而非过程编码的过程，能够从现有数据中学习以预测未来结果。

3.8 个人身份信息personally identifiable information，PII

任何（a）可用于识别与其相关的PII主体，或（b）是或可能直接或间接与PII主体相关联的信息。

注1；要确定PII主体是否可识别时，应考虑持有数据的隐私利益相关者或任何其他方可能合理使用的所有方法。

3.9 PII主体PII principal

个人身份信息（PII）所涉及的自然人

注1：根据管辖权和特定的数据保护和隐私法规，也可以使用同义词"数据主体"来代替术语"PII主体"。

4.组织环境

4.1理解组织及其环境

组织应确定与其意图相关的，且影响其实现数据治理管理体系预期结果能力的外部和内部事项。

4.2理解相关方的需求和期望

组织应确定：

a）数据治理管理体系相关方；

b）这些相关方与数据治理相关的要求。

注：相关方的要求可包括法律、法规要求和合同义务。

4.3确定数据治理管理体系的范围

组织应确定数据治理管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a）4.1中提到的外部和内部事项；

b）4.2中提到的要求；

c）组织实施的活动之间及其与其他组织实施的活动之间的接口与依赖关系。

该范围应形成文档化信息并可用。

4.4数据治理管理体系

组织应按照本标准的要求，建立、实现、维护和持续改进数据治理管理体系。

5领导

5.1领导和承诺

最高管理层应通过以下活动，证实其对数据治理管理体系的领导作用和承诺：

a）确保建立了数据治理策略和数据治理目标，并与组织战略方向一致；

b）确保将数据治理管理体系要求整合到组织过程中；

c）确保数据治理管理体系所需资源可用；

d）沟通有效的数据治理管理及符合数据治理管理体系要求的重要性

e）确保数据治理管理体系达到预期结果；

f）指导并支持相关人员为数据治理管理体系的有效性做出贡献；

g）促进持续改进；

h）支持其他相关管理角色，以证实他们的领导角色应用于其责任范围。

5.2方针

最高管理层应建立数据治理管理体系方针，该方针应：

a）与组织意图相适宜；

b）为设定数据治理目标提供框架；

c）包括对满足适用的数据治理相关要求的承诺；

d）包括对持续改进数据治理管理体系的承诺。

数据治理管理体系方针应：

e）形成文件化信息并可用；

f）在组织内得到沟通；

g）适当时，对相关方可用。

5.3组织的角色、职责和权限

最高管理层应确保与数据治理相关岗位的责任和权力在组织内得到分配和沟通。

最高管理层应分配责任和权限，以：

a）确保数据治理管理体系符合本标准的要求；

b）向最高管理者报告数据治理管理体系绩效。

注：最高管理层也可为组织内报告数据治理管理体系绩效，分配责任和权限。

6.规划

6.1应对风险和机遇的措施

6.1.1在规划数据治理管理体系时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机遇，以：

a）确保数据治理管理体系可达到预期结果；

b）预防或减少不良影响；

c）达到持续改进。

组织应规划：

d）应对这些风险和机遇的措施；

e）如何：

1）将这些措施整合到数据治理管理体系过程中，并予以实现；

2）评价这些措施的有效性。

6.2数据治理目标及其实现策划

6.2.1组织应在相关职能和层次上建立数据治理目标。

数据治理目标应：

a）与数据治理管理体系方针保持一致；

b）可测量（如果可行）；

c）考虑适用的要求；

d）得到监视；

e）得到沟通；

f）适时更新。

组织应保留有关数据治理目标的成文信息。

6.2.2规划如何实现数据治理目标时，组织应确定：

a）要做什么；

b）需要什么资源；

c）由谁负责；

d）何时完成；

e）如何评价结果。

7支持

7.1资源

组织应确定并提供建立、实现、维护和持续改进数据治理管理体系所需的资源。

7.2能力

组织应：

a）确定在组织控制下从事会影响数据治理管理体系绩效的工作人员的必要能力；

b）确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c）适用时，采取措施以获得必要的能力，并评价所采取措施的有效性；

d）保留适当的成文信息作为能力的证据。

注：适用措施可包括：例如针对现有雇员提供培训、指导或分配；雇佣或签约有能力的人员。

7.3意识

在组织控制下工作的人员应理解：

a）数据治理管理体系方针；

b）数据治理目标；

c）他们对数据治理管理体系有效性的贡献，包括改进绩效的益处；

d）不符合数据治理管理体系要求的后果。

7.4沟通

组织应确定与数据治理管理体系相关的内部和外部沟通，包括：

a）沟通什么；

b）何时沟通；

c）与谁沟通；

d）如何沟通；

e）由谁沟通。

7.5文件化信息

7.5.1总则

组织的数据治理管理体系应包括：

a）本文件要求的文件化信息；

b）为数据治理管理体系有效性，组织所确定的必要的文件化信息。

注：不同组织，数据治理管理体系文件化信息的详略程度可以是不同的，取决于：

1）组织的规模及其活动、过程、产品和服务的类型；

2）过程及其相互作用的复杂程度；

3）人员的能力。

7.5.2创建和更新

在创建和更新文件化信息时，组织应确保适当的：

a）标识和描述（如标题、日期、版本、作者或引用编号）；

b）格式（例如语言、软件版本、图表）和介质（例如纸质的、电子的）；

c）对适宜性和充分性的评审和批准。

7.5.3文件化信息的控制

数据治理管理体系及本标准所要求的文件化信息应得到控制，以确保：

a）在需要的地点和时间，是可用的和适宜使用的；

b）得到充分的保护（如避免保密性损失、不恰当使用、完整性损失等）。

为控制文件化信息，适用时，组织应进行以下活动：

a）分发、访问、检索和使用；

b）存储和防护，包括保持可读性；

c）变更控制（例如版本控制）；

d）保留和处置。

组织确定的为规划和运行数据治理管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

注：访问隐含着仅允许浏览文档化信息，或允许和授权浏览及更新文档化信息等决定。

8运行

8.1运行的规划和控制

组织应规划、实施和控制必要的过程以满足要求，并依据如下要求，实施第6章中确定的措施：

组织应保持文件化信息达到必要的程度，以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保外包过程是确定的和受控的。

8.2内部要求

数据的使用在所有行业和政府部门中的重要性日益突出，以至于组织必须将数据的使用纳入其总体战略之中，才能履行对各利益相关方的义务。

组织需要审视数据的潜在用途，既包括本组织自身的用途，也包括竞争对手的用途，并据此调整战略方向以实现预期成果；其中可能包括购买或出售数据。

组织内部将形成一种围绕数据使用的文化。组织必须塑造这种数据文化，确保其与实现总体目标所需的数据战略保持一致。由于数据的价值取决于据此作出的决策，这种数据文化应促使整个组织在数据获取、良好数据处理实践以及依赖相关情境下报告的各级决策流程等方面形成相应的行为规范。

8.3外部压力

组织可能需要调整其战略和政策，以确保符合所处市场的压力。此类市场压力包括：

a）客户对数据可用性、数据质量以及与现有数据互动方式的期望；

b）竞争对手利用数据改进或扩展其产品、服务或流程。

法律法规以及利益相关方要求在不同市场之间可能存在差异，组织必须确保其针对当前和未来数据使用所制定的战略和政策能够在这些市场中广泛适用。此类约束和义务可能适用于不同的数据问责活动，包括：

a）数据收集方式，包括围绕个人信息收集和使用的隐私告知与同意要求；

b）数据保留与处置要求；

c）在决策中妥善处理偏见、歧视和分析画像的义务；

d）数据共享或再利用所涉及的知识产权问题。

9监视、测量、分析和评价

9.1总则

织应确定：

a）需要被监视和测量的内容；

b）适用的监视、测量、分析和评价的方法，以确保得到有效的结果；

c）何时应执行监视和测量；

d）何时对监视和测量的结果进行分析和评价；

e）谁应分析和评价这些结果。

组织应保留适当的文件化信息，以作为监视和测量结果的证据。

9.2内部审核

9.2.1组织应按照计划的时间间隔进行内部审核，以提供信息，确定数据治理管理体系：

a）是否符合：

1）组织自身的数据治理管理体系的要求；

2）本标准的要求；

b）是否得到有效地实施和保持。

9.2.2组织应：

a）规划、建立、实现和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。

审核方案应考虑：

1）相关过程的重要性；

2）影响组织的变更；

3）以往审核的结果。

b）定义每次审核的审核准则和范围；

c）选择审核员并实施审核，确保审核过程客观性和公正性；

d）确保将审核结果报告给相关管理者；

e）保留文件化信息作为审核方案和审核结果的证据。

9.3管理评审

9.3.1总则

最高管理层应按计划的时间间隔评审组织的数据治理管理体系，以确保其持续的适宜性、充分性和有效性。

管理评审应考虑：

a）以往管理评审提出的措施的状态；

b）与数据治理管理体系相关的外部和内部事项的变化；

c）有关数据治理管理绩效的反馈，包括以下方面的趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果；

d）相关方反馈；

e）风险评估的结果及风险处置计划的状态；

f）持续改进的机会。

管理评审的输出应包括与持续改进机会相关的决定以及变更服务管理体系的任何需求。

组织应保留文档化信息作为管理评审结果的证据。

10.改进

10.1不符合及纠正措施

10.1.1当出现不符合时，组织应：

a）对不符合做出应对，并在适用时：

1）采取措施，以控制和纠正不符合；

2）处理后果；

b）通过下列活动，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方发生：

1）评审和分析不符合；

2）确定不符合的原因；

3）确定类似的不符合是否存在，或可能发生；

c）实现任何需要的措施；

d）评审所采取的纠正措施的有效性；

e）必要时，对数据治理管理体系进行变更。

纠正措施应与所遇到的不符合的影响相适应。

10.1.2组织应保留成文信息，作为下列方面的证据：

a）不符合的性质及所采取的任何后续措施；

b）任何纠正措施的结果。

10.2持续改进

组织应持续改进数据治理管理体系的适宜性、充分性和有效性