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。