ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

信息安全技术 数据安全评价
第1部分：要求

Information security technology-Data security evaluation-Part 1:Requirements

（征求意见稿）

（本草案完成时间：2021-04-18）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

DB21/T XXXX《信息安全技术 数据安全评价》已发布1个部分：

——第1部分：要求

本文件为DB21/T XXXX的第1部分。

本文件按照GB/T 1.1—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。

本文件由中共辽宁省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：大连软件行业协会、大连交通大学、大连华信计算机技术股份有限公司、大连奥远电子股份有限公司、辽宁省信息中心、大连理工现代工程检测有限公司、大连市计算机学会。

本文件主要起草人：郎庆斌、尹宏、刘宏、胡剑锋、杨万清、杨莉、于青、才昊、司丹、孙毅、王小庚。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市和平区光荣街26号甲，联系电话：024-81680033

本文件起草单位通讯地址：大连市高新园区火炬路32号创业大厦A座5层，联系电话：0411-83655207

信息安全技术 数据安全评价
第1部分：要求

1 范围

本文件规定了数据安全评价的管理、指标、流程、准备、申请受理、现场审核、审批和公示、仲裁服务、人员管理、文档管理、过程管理和资格管理等的规范。

本文件适用于各类数据安全评价机构，亦为已建立数据安全管理体系的个人、企业、事业、社会团体等组织提供参照。

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。

DB21/T 1628.1 信息安全 个人信息保护规范

DB21/T 1628.2 信息安全 个人信息安全管理体系实施指南

DB21/T XXXX 信息安全技术 数据管理规范

3 术语和定义

DB21/T 1628.1、DB21/T XXXX界定的以及下列术语和定义适用于本文件。

3.1

数据安全评价 data security evaluate

由独立、公正的第三方评价机构，基于相关法律、标准，系统、全面、客观地审查、判断、评估数据安全状况的权威、有效活动。

4 缩略语

下列缩略语适用于本文件。

DSE：数据安全评价（Data Security Evaluate）

5 评价管理

5.1 评价原则

5.1.1 以用户为中心

应充分理解用户需求，关注用户业务流程，使评价客观、全面、整体、有效。

5.1.2 基于事实管理

应保证获得数据、信息的可靠性、准确性，基于事实科学、客观分析、判断、评估。

5.1.3 质量管理

应采用PDCA过程管理模式，保证评价质量和评价的权威性。

5.1.4 持续改进

应不断改进、完善评价体系，提高评价体系的有效性，以更加适应用户、社会的需要。

5.2 评价组织

5.2.1 要求

实施DSE，应建立相应的工作机制和评价机制，以管理、约束DSE相关活动、行为。

5.2.2 工作机制

5.2.2.1 构成

建立工作机制，是为推进数据安全、实施DSE设立的专门的组织机构：

a) 应包括主管机构、相关行业、相关企业代表，及专家、学者和相关研究人员；
b) 应设立若干职能单元，履行各项管理职能，如法规、仲裁、宣传、教育培训；
c) 组建 DSE 的管理、实施机构，推进 DSE 工作等。

5.2.2.2 职能

设立工作机制的职能，主要应包括：

a) 推进、实施数据安全相关工作；
b) 推进数据安全管理体系建设；
c) 研究、制定、解释、修改、实施数据安全相关法规、标准；
d) 研究、制定、解释、修改、实施 DSE 相关标准、规则；
e) 监督 DSE 管理、实施机构的工作；
f) 审计 DSE 管理、实施相关活动和文档；
g) 推进数据安全、DSE 相关宣传、培训、教育；
h) 建立争端解决仲裁机制等。

5.2.3 评价机制

5.2.3.1 构成

DSE机制是数据安全评价工作机制为管理、实施DSE组建的专门机构：

a) 评价机制的构成应包括专家、学者、专业人士和管理人员等；
b) 评价机制应设立常设机构，如评价办公室。

5.2.3.2 职能

评价机制的职能，主要应包括：

a) 评价人员管理
   1) 评价人员审查、聘任；
   2) 评价人员培训、考核；
   3) 评价人员职责和义务；
   4) 评价人员派出和管理；
   5) 评价人员相关事务管理。
b) 评价事务管理
   1) 接受 DSE 申请；
   2) 审查 DSE 资格；
   3) 审核申请 DSE 提交资料；
   4) 现场审核数据安全管理体系；
   5) 提交 DSE 相关文档；
   6) 数据安全评价复审；
   7) 发放 DSE 证书；
   8) 其它 DSE 相关事务。
c) 评价质量控制
   1) 评价人员评估；
   2) 评价过程评估；
   3) 评价效果评估；
   4) 其它质量相关因素评估。
d) 仲裁服务
   1) 制定投诉处理规则；
   2) 建立投诉处理流程；
   3) 建立投诉受理和反馈机制；
   4) 明确投诉处理人员的职责和义务；
   5) 建立投诉监督机制；
   6) 特殊情况处理等。
e) 培训教育
   1) 制订培训教育计划；
   2) 确定培训教育方式、方法；
   3) 选择适宜的培训教育教材；
   4) 明确培训教育师资及相应的职责和义务；
   5) 培训教育考核；
   6) 培训教育效果评估。
f) 文档管理
   1) 编制 DSE 资格审核报告；
   2) 编制 DSE 现场审核报告；
   3) 编制 DSE 报告；
   4) 编制 DSE 整改报告；
   5) 建立 DSE 相关文档管理制度；
   6) 其它 DSE 相关文档的管理。

g) 日常事务管理
   1) 建立评价机制的相关管理制度；
   2) 日常事务处理；
   3) 受理 DSE 相关意见、建议、投诉；
   4) 其它 DSE 相关事务。

5.3 评价体系

为保证DSE的质量，应建立相应的评价体系。评价体系主要应包括：

a) 评价对象和评价目的；
b) 评价机制的管理；
c) 评价人员管理；
d) 评价方法和手段；
e) 评价指标；
f) 评价流程；
g) 评价过程管理；
h) 评价质量管理；
i) 评价结果管理等。

6 评价指标

6.1 要求

为保证DSE的科学性、规范性，设计并建立DSE指标体系，并融合数据管理者的管理特征，应：

a) 依据 DB21/T 1628.1，充分考虑个人信息管理特征、个人信息安全与一般数据安全的差异；
b) 依据 DB21/T XXXX，充分考虑一般数据的管理特征、数据管理与个人信息管理的差异、安全特征差异等；
c) 在 DSE 指标体系内统一描述特征差异等。

6.2 设计

6.2.1 要求

DSE指标设计，应考虑：

a) 应全面、整体评估、判断数据管理者特征、数据管理特征；
b) 应全面、整体评估、判断 DSMS、体系内各个功能要素之间的关联关系；
c) 应合理设计评价指标，关注评价指标之间、评价指标项之间的关联关系，避免雷同、重复、矛盾；
d) 应基于数据管理者实际需求，真实、客观、准确地反映数据安全状况等。

6.2.2 结构

DSE指标结构，应包括：

a) 应基于 6.1 的要求，设计评价指标整体框架，由通用的 DSE 指标构成；
b) 应基于数据管理者实际需求，设计 DSE 指标的指标项；

c） 应根据数据管理者特殊需求，设计 DSE 指标和相应的指标项。

注：参看DB21/T XXXX.4 信息安全技术 数据安全评价 第4部分：评价指标

6.3 评估

应在DSE的全生命周期评估DSE指标的科学性、合理性、可用性和有效性，随时修正、完善并持续改进。

7 评价流程

评价流程如图1示。

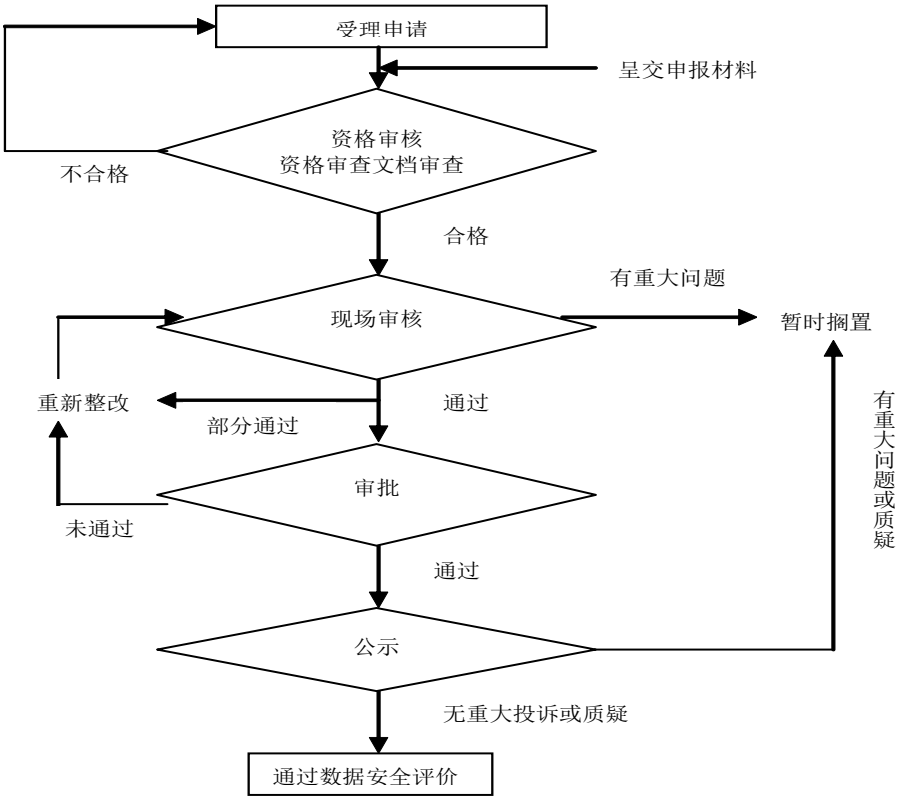

图1 评价流程

8 评价准备

8.1 管理体系

应依据DB21/T 1628.1、DB21/T XXXX，建立DSMS，在法规、标准框架内实施数据管理；

应依据DB21/T 1628.1、DB21/T XXXX，展开DSMS内审，持续改进、完善DSMS。

8.2 内审

应实施数据管理内审，或在DSMS运行3个月后实施DSMS内审：

a) 依据 DB21/T 1628.1、DB21/T XXXX 标准，检查、评估数据管理、DSMS 实施、运行状况；
b) 依据 DB21/T 1628.1、DB21/T XXXX 标准，评估数据管理、DSMS 内审结果；
c) 依据相关法规、标准，评估数据管理、DSMS 与业务需求的融合度；
d) 判断、评估数据管理与相关法规、标准的符合性、一致性和有效性；
e) 数据管理、DSMS 缺陷整改措施和有效性；
f) 申请 DSE 的可行性等。

8.3 申报准备

申请DSE，应根据评价实施机构要求，准备相应的资格审核材料：
a) DSE 申请；
b) 数据管理者基本情况说明；
c) 数据管理说明；
d) DSMS 实施、运行情况说明；
e) 数据管理、DSMS 相关文档；
f) 数据管理、DSMS 内审报告；
g) 其它需要说明的问题等。

9 申请受理

9.1 资格审核

9.1.1 要求

评价实施机构受理DSE申请，应审核申请者的资格。资格审核应包括资格审查和文档审查。

9.1.2 资格审查

评价实施机构应依据DB21/T 1628.1、DB21/T XXXX和其它数据安全相关法规、标准，审核申请DSE的数据管理者的申请资格。审查内容主要应包括：
a) 数据管理者的合法性；
b) 数据管理者的业务相关性；
c) DSMS 相关文档的规范性、完整性，包括：
    1) 数据管理相关文档；
    2) DSMS 内审报告：
    3) 数据管理、DSMS 运行状况评估；
    4) 数据管理、DSMS 整改措施和相关报告；
    5) 数据安全相关事故报告；
    6) 其它需要提供的文档。
d) 其它需说明的问题。

9.1.3 文档审查

9.1.3.1 审查条件

评价实施机构应依据DB21/T 1628.1、DB21/T XXXX和其它数据安全相关法规、标准，审查申请DSE的数据管理者提交的数据管理、DSMS相关文档。审核者应符合条件：

a) 审核应由评价实施机构聘请的相关专业评价人员实施；
b) 审核前应明确审核人员的职责和要求；
c) 申请评价的数据管理者与审核人员无直接关系；
d) 应制定审核控制要求和记录要求等。

9.1.3.2 审查内容

文档审查的主要内容，应包括：

a) 评估提交的相关文档的真实性、有效性；
b) 评估提交的相关文档内容的规范性、完整性；
c) 根据文档初步评估数据管理、DSMS 实施、运行状况；
d) 评估数据管理与数据安全相关标准、法规的符合性；
e) 评估个人信息与一般数据管理的统一性和有效性；
f) 质疑可能存在的问题，并明确结果。

9.2 审核结论

9.2.1 审核合格

资格审核满足下列条件的，应予合格：

a) 数据管理、DSMS 相关文档规范、完整、真实、有效；
b) 数据管理、DSMS 实施、运行状况良好；
c) 数据管理有效，符合数据安全相关标准、法规；
d) 数据管理、DSMS 运行存在可接受的非实质性问题。

9.2.2 基本合格

资格审核符合下列条件的，应要求数据管理者修改、改进、完善后重新提交审核：

a) 数据管理、DSMS 相关文档存在缺陷，需要改进、完善；
b) 数据管理、DSMS 实施、运行存在某些需要改进、完善的问题；
c) 存在某些需要现场评价确认的一般性问题。

9.2.3 不合格

资格审核中发现存在下列问题，评价实施机构应退回申报材料，并要求数据管理者重新内审，达到评价要求后重新申请：

a) 数据管理、DSMS 相关文档存在重大隐患（如虚报、瞒报等）；
b) 数据管理、DSMS 实施、运行存在重大缺陷；
c) 发生重大数据安全事故，且存在下列情况之一：
    1) 事故等级较高；
    2) 事故处理措施不当；
    3) 尚在恢复期。

9.3 审核报告

评价实施机构完成资格、文档审查后，应编制资格审核报告，主要内容应包括：

a) 数据管理者基本情况审查说明；
b) 数据管理者提交文档审查情况说明；
c) 初步评估数据管理、DSMS 实施、运行状况；
d) 数据安全相关法规、标准的符合性；
e) 不符合、不满足 DSE 要求事项说明；
f) 符合基本合格要求的数据管理者出具的整改报告；
g) 审核结论等。

10 现场审核

10.1 审核组织

10.1.1 审核组

资格审核合格后，评价实施机构应组建DSE现场审核组，实地判断、评估数据管理者数据管理、DSMS实施、运行状况。

10.1.2 审核计划

现场审核组组长应根据资格审核报告、数据管理者实际和DB21/T 1628.1、DB21/T XXXX及相关法规、标准等编制DSE现场审核计划：

a) 数据管理者基本信息；
b) 资格审核报告说明；
c) 现场审核组的职能、职责；
d) DSE 现场审核重点；
e) DSE 现场审核方法；
f) DSE 现场审核有效性验证；
g) DSE 现场审核安全性保证；
h) DSE 现场审核文档管理等。

10.2 审核会议

10.2.1 要求

在DSE现场审核中，审核组应以会议的形式完成现场审核准备，及审核组内部、审核组与数据管理者之间的沟通、交流、说明等。

10.2.2 审核准备

审核组应在进入现场前召开全体审核人员会议，说明DSE现场审核计划，明确DSE现场审核的目的和任务。

10.2.3 进入现场

审核组应在进入现场后召开由审核人员、数据管理者最高责任人、数据管理相关责任人参加的工作会议。会议内容应包括：

a) 依据 DB21/T 1628.1、DB21/T XXXX 及相关法规、标准，说明 DSE 的目的；
b) 说明 DSE 现场审核计划；
c) 说明 DSE 现场审核要求；
d) 说明 DSMS 原始文档收集要求；
e) 说明 DSE 现场审核抽样方法；
f) 确认 DSE 现场审核所需资源；
g) 澄清可能存在的问题；
h) 数据管理者准备情况说明。

10.2.4 审核过程

审核组应在DSE现场审核过程中适时召开工作例会，会议内容应包括：
a) 及时通报、沟通、交流现场审核信息；
b) 及时研究、讨论现场审核中无法确认、含糊不清等问题；
c) 形成一致、统一的结论。

10.2.5 审核结束

审核组应在现场审核结束后召开由审核人员、数据管理者最高责任人、数据安全相关责任人参加的工作会议，会议内容应包括：
a) 依据 DB21/T 1628.1、DB21/T XXXX 及相关法规、标准，说明 DSE 的目的；
b) 说明 DSE 现场审核计划执行情况；
c) 说明 DSE 现场审核抽样方法；
d) 解释、说明 DSE 现场审核发现的问题；
e) 数据管理者应澄清或确认审核组提出的问题；
f) DSMS 实施、运行状况判断、评估说明；
g) 明确说明 DSE 现场审核意见；
h) 说明 DSMS 修正、完善、改进要求和建议；
i) 说明 DSE 现场审核意见存在疑义的申诉过程；
j) 说明 DSE 现场审核事后监督程序等。

10.3 调查方法

10.3.1 面谈

现场审核人员应根据现场审核准备阶段确定的审核目标、审核内容及资格审查中需要确认的问题，设计面谈样本，并依据样本分别访问相关人员。面谈方式可包括：
a) 集体面谈：与 DSMS 相关责任人集体访谈，调查并确认 DSMS 运行状况；
b) 个人面谈：根据调查内容选择适宜的样本人员，调查个人对数据安全的理解和 DSMS 对个人的影响；
c) 客户面谈：宜与数据管理者的相关客户接触，调查客户对数据管理状况的认知和 DSMS 对客户的影响等。

注：面谈应与其它调查方法结合使用。

10.3.2 文档检查

审核组应依据DB21/T1628.2、DB21/T XXXX，检查数据管理相关文档、DSMS相关文档的原始纪录和资料，调查并确认数据管理机制的状况。

10.3.3 抽样调查

10.3.3.1 要求

审核组应根据面谈、文档检查结果，选取适宜的样本，调查DSMS实施、运行状况。

10.3.3.2 样本选择

选择抽查样本，一般考虑：

a) 业务流程：应选择典型的、与数据安全相关的重点业务流程；
b) 易忽视环节：应注意选择在数据管理中易忽视或存在缺陷的薄弱环节；
c) 高风险环节：应选择具有高风险的数据管理、处理、使用环节；
d) 异常现象：应选择 DSE 过程中存在疑问或异常的事件等。

10.3.3.3 抽样范围

确定抽样范围，一般考虑：

a) 应包括时间范围、样本选择范围、样本检查范围等；
b) 应依据 DB21/T1628.2、DB21/T XXXX 及相关法规和标准、DSMS 现场审核计划和数据管理者的实际，以及 DSMS 实施、运行状况确定等。

10.3.3.4 抽样数量

抽样数量应保证抽查样本可以反映数据管理的总体特征，并相对准确，以提高现场审核效率。确定抽样数量，一般考虑：

a) 规模：抽样数量可根据数据管理者的规模确定；
b) 实际状况：应根据数据管理的重视程度、DSMS 实施运行的有效性确定；
c) 缺陷：应根据数据管理和 DSMS 实施运行的缺陷和薄弱环节确定。

10.3.3.5 抽查结论

抽样调查结束后，应形成抽样调查结论。一般应考虑：

a) 不能确定的问题，不应轻易做出结论；
b) 发现的缺陷、漏洞等，应具有充足的证据；
c) 结论不应绝对化，应根据数据安全相关法规、标准形成。

10.4 审核实施

10.4.1 要求

现场审核实施要求包括：

a) 现场审核人员要求：
    1) 现场审核人员应科学、专业、客观地分析、判断、评估 DSMS 运行状况；
    2) 现场审核人员不应根据个人好恶主管臆断，有悖事实；
    3) 现场审核人员应从全局角度综合判断、评估分工范围内的数据管理状况。

b) 调查样本人员要求：

接受调查的样本人员应真实、客观地说明相关问题，避免自身利益考虑或忽视事实的情况。

10.4.2 审核质量

10.4.2.1 要求

应在DSE现场审核中实施质量控制，避免和减少调查偏差，以真实反映数据管理者的数据安全状况。

10.4.2.2 控制措施

在现场审核中，应采取相应的控制措施，保证现场审核质量，主要包括：

a) 应基于资格审核明确现场审核的目的和要求；
b) 应明确现场审核任务、内容和问题，设计现场审核方案和现场调查表；
c) 应选择恰当、组合的调查方法，依据现场审核方案制定相应的审核大纲；
d) 应保证现场调查表的设计质量：
   1) 应符合数据安全相关法规、标准和数据管理者的实际；
   2) 调查问题应简单明了、易于理解；
   3) 调查问题应选择固定答案；
   4) 说明性答案应简洁并可反映问题的实质等。
e) 应采用科学方法，定性或定量分析现场调查取得的相关信息，并说明数据管理现状、缺陷、漏洞、隐患和影响等。

10.4.2.3 问题处理

在现场审核过程中，应及时处理影响DSMSE质量的各种问题：

a) 应适时召开工作例会，分析、研究、讨论不明确的、无法确认的或含糊不清的问题，及时发现严重的或潜在的问题；
b) 应重新检查、审核不能确认的调查证据；
c) 应验证资格审核中提出的问题。

10.4.3 调查偏差

在现场调查中，应注意偏差控制，避免或减少各种原因引起的偏差：

a) 偏差类型：
   1) 整体偏差：在现场审核的各个环节均可能出现的偏差；
   2) 随机偏差：在抽样调查中可能出现的偏差。
b) 偏差原因：可能造成偏差的原因包括：
   1) 面谈提问；
   2) 审核双方的心理状态；
   3) 调查文档的设计质量和填写质量；
   4) 调查分析的主观因素；
   5) 抽查样本的选择；
   6) 沟通、交流不充分等。

10.4.4 沟通交流

在现场审核过程中，应与数据管理者充分沟通、交流，了解审核对象的观点，清晰、明确、具有说服力的阐明现场审核的分析、判断、评估观点。

10.5 审核结论

10.5.1 要求

DSE现场审核结束后，现场审核组应整理、分析、判断、评估现场调查中累积的所有相关信息，清楚、明确地说明数据管理的问题，形成客观、真实、公正的审核意见。

10.5.2 问题分类

现场审核中发现的问题，主要应分为2大类：

a) 严重问题：以下问题应视为严重问题：
   1) 实际情况与申报资料不符（隐瞒事实、虚报、瞒报等）；
   2) 存在严重的数据安全隐患（或经整改后仍不能达到数据安全要求）；
   3) 出现严重的数据安全事故等。
b) 一般问题：以下问题应视为一般问题：
   1) 因未充分理解 DSE 要求出现的申报资料不规范、内容不完整等情况；
   2) 存在一般性的数据安全隐患，经整改可在短期内达到数据安全要求；
   3) 其它非实质性问题。

10.5.3 审核意见

现场审核意见应分为3种：

a) 通过现场审核：
   1) 数据管理严谨、规范，DSMS 实施、运行安全、可靠，符合数据安全相关法规、标准和 DSE 要求，满足数据主体的数据安全需求；
   2) 存在少量一般性问题，经简单改进、修正，可基本符合数据安全相关法规、标准和 DSE 要求，满足数据主体的数据安全需求。
b) 整改后通过现场审核

存在短期内可修改、纠正的非实质问题，应经整改后再次申请现场审核，如基本符合数据安全相关法规、标准和DSE要求，满足数据主体的数据安全需求，且问题已经修正。

c) 不能通过现场审核：
   1) 存在严重问题，不符合数据安全相关法规、标准和 DSE 要求，完全不能满足数据主体的数据安全需求；
   2) 存在短期内可修改、纠正的非实质问题，但经过整改后再次现场审核仍不能达到数据安全相关法规、标准和 DSE 要求。

10.6 整改

10.6.1 整改意见

现场审核组应以工作例会的形式，分析、研究、判断、评估问题存在的根本原因，确定问题的性质和分类，形成一致的、符合事实的整改意见，并提出适合的改进措施和解决方案。

10.6.2 整改报告

现场审核完成后，存在10.5.3 a）2）、b）问题的数据管理者，应在问题解决后形成整改报告，主要内容应包括：

a） 问题说明；
b） 整改措施和方法；
c） 内审报告；
d） 自评结果和说明；
e） 其它需说明的事项。

10.7 现场审核报告

DSE现场审核完成后，应形成现场审核报告，主要内容应包括：

a） 数据管理者情况说明；
b） DSMS 实施、运行状况；
c） 现场审核过程说明；
d） 问题说明和分析；
e） 现场审核结论和说明；
f） 建议和意见等。

11 审批和公示

11.1 审核

DSE现场审核结束后，现场审核组应将资格审核报告、现场审核报告等DSE相关文档提交评价机构审核，审核内容主要应包括：

a） DSE 是否符合数据安全相关法规、标准；
b） DSE 依据是否充分、有效；
c） DSE 方法是否适当、合理；
d） 现场审核中收集的信息是否典型、齐全；
e） 资格审核、现场审核结论是否适当、正确；
f） 文字描述是否准确等。

11.2 评价报告

评价机构审核通过后，应由现场审核组编制DSE报告。评价报告内容主要应包括：

a） 数据管理者情况说明；
b） 资格审核报告说明；
c） 现场审核报告说明；
d） 整改报告说明；
e） 评价结论认定和说明；
f） 评价分析说明等。

11.3 审批

评价报告完成后，应报DSE相关工作机制审批，并签署审批意见。如未通过审批，数据管理者应整改后重新申请现场审核。

11.4 公示

DSE通过审批后，应通过适当方式公示：

a) 如公示期内无重大投诉、质疑，应正式通过 DSE，并发布公告；
b) 如公示期内出现重大投诉、质疑，且经证实，应取消相应的 DSE 申请资格，并经整改后重新申请。

12 仲裁服务

评价机构应提供仲裁服务，处理DSE相关的投诉、意见、建议和相应的反馈。主要应包括：

a) 制定投诉处理规则；
b) 建立投诉处理流程；
c) 明确投诉受理人的职责和义务；
d) 建立投诉受理和反馈机制；
e) 建立意见和建议的受理和反馈机制；
f) 建立监督机制；
g) 建立特殊情况处理机制；
h) 其它必须的事项。

13 人员管理

13.1 要求

评价机制常设机构应建立DSE人员的管理机制，以保证DSE的质量、专业、效果。

13.2 构成

DSE人员应包括IT、信息安全、管理等相关领域及相关行业或领域的专家、学者、专业技术人员和社会人士。

13.3 资格

DSE人员，应根据业务能力、专业能力和从业经验等划分不同的评价资格等级，并明确相应的评价能力。

13.4 制度

评价机制常设机构应建立DSE人员管理制度，以保证DSE的权威性、独立性。主要应包括：

a) 资格认定；
b) 职责和义务；
c) 行为规范；
d) 资格等级等。

13.5 培训

13.5.1 计划

评价机制常设机构应根据不同评价资格等级的评价人员能力要求制定相应的DSE相关的培训教育计划。

13.5.2 内容

评价机制常设机构实施评价人员相关知识培训，主要应包括：

a) 数据安全相关法规、标准；
b) 数据安全相关知识；
c) 数据管理；
d) DSMS 相关知识；
e) DSE 的基本知识；
f) DSE 基本方法等。

13.5.3 方式

DSE培训教育，宜采用2种培训方式：

a) 定期：
   1) 根据培训教育计划定期实施；
   2) 根据 DSE 过程中的问题定期、实时实施。
b) 研讨：
   1) 评议 DSE 过程；
   2) 针对典型案例、有争议问题，或设定课题讨论。

14 文档管理

14.1 记录

应在DSE过程中记录所有与评价活动和行为相关的信息，包括目的、依据、时间、对象、人员、方式方法、和过程等。

14.2 文档

应在DSE过程的各个阶段形成相应的文档，包括计划、大纲、表格、报告等。

14.3 备案

应建立与DSE相关的记录、文档、规章、文件、合同等的备案管理制度，并应根据实际需要改进和完善。

15 过程改进

15.1 过程模式

应在DSE过程中分析、发现DSE流程存在的缺陷，并采用PDCA模式，修正、改进。

15.2 持续改进

应通过过程改进，分析DSE目标、结果、过程和相关资料，发现DSE的体系缺陷，持续改进，以提高DSE的有效性。

16 资格管理

16.1 要求

通过DSE的数据管理者，应履行数据管理的职责和义务，基于PDCA模式，持续改进、完善DSMS，保障数据主体权益；评价机制常设机构应审计、监督、管理通过DSE的数据管理者，定期复查、复审，以保证评价效果的持续性、实效性。

16.2 监督检查

评价机制常设机构应定期抽查通过DSE的个人信息管理者，并监督抽查不合格的数据管理者整改：

a) 合格：数据管理工作持续、有效，DSMS 运行安全、可靠，且持续改进、完善；
b) 不合格：数据管理者通过 DSE 后，数据管理工作停滞，DSMS 不能持续改进、完善，数据主体权益存在安全风险，应限期整改；
c) 整改后不合格：抽查不合格的数据管理者，限期整改后仍不能满足数据安全相关法规、标准和 DSE 要求，则应取消相应的 DSE 申请资格，并限定整改周期，经整改后重新申请。

16.3 复审

数据管理者通过DSE后，评价机制常设机构应根据不同情况复审：

a) 应在通过 DSE 后定期复审；
b) 数据管理者更名、法人变更、义务变化、办公场所更换等，应重新申请现场审核；
c) 数据管理者通过 DSE 后，出现数据安全重大事故，应通过复审确认，取消相应的 DSE 申请资格，并限定整改周期，经整改后重新申请；
d) 数据管理者通过 DSE 后，评价机制常设机构接到投诉，质疑数据管理的重大失误、缺陷等，应通过复审确认，取消相应的 DSE 申请资格，并限定整改周期，经整改后重新申请。