ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX.2—XXXX

信息安全技术 数据安全评价 第2部分：管理指南

Information Security technology-data security evaluation part2：management guidelines

（征求意见稿）

（本草案完成时间：2023-1-10）

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 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　要求 1
5　评价 2
5.1　相关方 2
5.2　对象 3
6　评价组织 3
6.1　要求 3
6.2　管理主体 3
6.3　工作机构 4
6.4　评价机构 5
6.5　职责 6
6.6　管理 7
6.7　工作流程 7
7　评价管理 8
7.1　概述 8
7.2　评价边界 8
7.3　组织 9
7.4　控制 9
7.5　协调 9
8　评价体系 9
8.1　评价要素 9
8.2　评价规则 10
8.3　评价等级 10
8.4　评分范围 10
8.5　构建DSE体系 10
9　评价指标 11
9.1　概述 11
9.2　设计 11
9.3　评估 11
10　过程管理 12
10.1　要求 12
10.2　管理机制 12
10.3　评价机构 12

10.4 评价实施.....12
10.5 审批和公示.....13
10.6 仲裁服务.....14
11 人员管理.....14
12 文档管理.....14
13 过程改进.....14
14 资格管理.....14

前　言

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。

本文件是DB21/T XXXX《信息安全技术 数据安全评价》的第2部分。DB21/T XXXX已经发布了以下部分：

——信息安全技术 数据安全评价 第1部分：要求
——信息安全技术 数据安全评价 第2部分：管理指南
——信息安全技术 数据安全评价 第3部分：审核员管理
——信息安全技术 数据安全评价 第4部分：评价指标
——信息安全技术 数据安全评价 第5部分：评价方法
——信息安全技术 数据安全评价 第6部分：资格审核
——信息安全技术 数据安全评价 第7部分：现场管理
——信息安全技术 数据安全评价 第8部分：保证方法
——信息安全技术 数据安全评价 第9部分：仲裁管理
——信息安全技术 数据安全评价 第10部分：审批管理
——信息安全技术 数据安全评价 第11部分：资格管理

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：大连软信咨询服务有限公司、国家计算机网络应急技术处理协调中心辽宁分中心、大连交通大学、大连理工现代工程检测有限公司、大连软件行业协会、大连市计算机学会。

本文件主要起草人：郎庆斌、李凯、才昊、孙鹏、尹宏、秦健、宋悦、杨莉、司丹、孙毅、曹剑、王小庚、王鑫。

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2部分：管理指南

1 范围

本文件规定了数据安全评价相关方、对象、评价组织、评价管理、评价体系、评价指标、过程管理、人员管理、文档管理、过程改进、资格管理等相关要求。

本文件适用于为构建数据安全评价的评价体系、评价管理、评价规则，及数据安全评价实施提供指导和通用规则。

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 XXXX 信息安全技术 个人信息安全 术语

DB21/T 1628.1 信息安全技术 个人信息安全 第1部分：要求

DB21/T 1628.2 信息安全技术 个人信息安全 第2部分：实施指南

DB21/T XXXX 信息安全技术 数据管理规范

DB21/T XXXX.1 信息安全技术 数据安全评价 第1部分：要求

3 术语和定义

DB21/T XXXX、DB21/T XXXX、 DB21/T XXXX.1界定的以及下列术语和定义适用于本文件。

3.1

评价 evaluation

事物的分析、判断和评估。

3.2

主体 principal part

具有法人资格并承担相应责任和义务的组织机构。

3.3

评价主体 evaluation of principal part

依法取得法人资格并具有相应资质，获得数据管理机构认可，独立从事DSE活动的机构。

4 要求

本文件遵循DB21/T XXXX.1确立的DSE的基本原则和要求，重点描述和指导DSE的管理和实施。

管理、实施DSE，应以DB21/T 1628系列标准和DB21/T XXXX为基准。

管理、实施DSE，应同时使用DB21/T XXXX.1和本文件，并参照DB21/T XXXX（评价）系列其它标准。

管理、实施DSE，亦应同时融合、参照信息安全、质量管理、服务管理等其它标准体系。

5 评价

5.1 相关方

5.1.1 第一方

DSE的第一方应是数据（个人信息）管理者。

a) 数据（个人信息）管理者应通过内审和过程管理，保证 DSMS（PISMS）的有效、安全和可靠，提高数据（个人信息）管理者的信用保证；
b) 数据（个人信息）管理者应遵循 DB21/T 1628.2 第 9 章、DB21/T XXXX 第 6 章的规则；
c) 数据（个人信息）管理者应获得评价主体的评价认可等。

5.1.2 第二方

DSE的第二方应是个人信息主体。

a) 数据（个人信息）管理者管理数据（个人信息）的合理、有效、充分，及数据（个人信息主体）权益的保障，应由权威、有信誉的评价主体提供保证；
b) 数据（个人信息）主体的权力和义务应遵循 DB21/T 1628.1 第 6 章、DB21/T 1628.2 第 7 章、DB21/T XXXX 第 5 章的规则；
c) 数据（个人信息）主体应通过 DSE 认知数据（个人信息）管理者的管理能力和服务质量。

5.1.3 第三方

5.1.3.1 主体

DSE的第三方应是评价机构，是从事DSE的评价主体，应包括以下特征：

a) 合法、有效、独立并具有相应资质的法人组织；
b) 独立行使法定权力，承担社会责任和法律义务；
c) 获得管理机构的认可；
d) 有固定的工作环境和必要的相关设备、设施等及相应的技术能力；
e) 依据 DB21/T XXXX.1 4.2.3，具备评价机构职能和相应的管理制度、管理机制；
f) 具有 DB21/T XXXX.1 第 12 章规定的评价人员规则和相应的管理制度、管理机制；
g) 评价机构的最高管理者、各级责任主体应具备履行 DSE 必备的知识、能力、责任、义务等；
h) 具有取得评价能力认定的专职高、中、低级评价人员配备；
i) 依据数据（个人信息）安全相关法规、标准应具备的其它条件等。

5.1.3.2 责任和义务

5.1.3.2.1 责任

评价主体应承担的责任主要应包括：

a) 社会责任：
    1) 客观、真实的事实判定；
    2) 权威、有信誉的质量保证；
    3) 获得第一方和第二方充分信任的信用保证；
    4) 引导行业自律，保护数据（个人信息）主体权益；
    5) 评价相关方的协调、沟通；
    6) 提供安全策略和相应建议等。

b) 法律责任：
评价主体应承担和履行评价过程中保证数据（个人信息）安全的法律责任，避免因评价引发数据（个人信息）主体权益受损。

5.1.3.2.2 义务

评价主体应承担的相应义务主要应包括：

a) 社会义务：为承担和履行社会责任，保证评价的客观、公正、公平展开的评价相关的活动；
b) 法律义务：为承担法律责任，保证评价质量和数据（个人信息）主体权益所应遵循的相关法规、标准。

5.2 对象

5.2.1 数据（个人信息）管理者

数据（个人信息）管理者是数据（个人信息）的管理主体，应遵循DB21/T 1628.1第6章、DB21/T 1628.2第7章、DB21/T XXXX第5章的规定，以保证个人信息管理的安全、规范、有效。

5.2.2 数据（个人信息）管理

数据（个人信息）管理是数据（个人信息）管理者向数据（个人信息）主体提供服务的过程，应遵循DB21/T 1628.1、DB21/T 1628.2、DB21/T XXXX的约束规则，保证个人信息安全。

5.2.3 DSMS（PISMS）

DSMS（PISMS）应是DSE的对象，其主要特征应包括：

a) 数据（个人信息）管理者的基本状态；
b) 数据（个人信息）管理的特征、属性；
c) 数据（个人信息）管理的策略、机制；
d) 数据（个人信息）管理的过程、质量控制；
e) 数据（个人信息）管理的安全风险评估等。

6 评价组织

6.1 要求

评价组织应考虑：

a) DB21/T XXXX.1 4.2 确立的评价组织规则，应是 DSE 的组织保障，应首先依据 DB21/T XXXX.1 4.2 组建；
b) 管理机构应依据 DB21/T XXXX.1 4.2 设置 DSE 管理的相关职能单元，以保证 DSE 的规范性、科学性；
c) 评价主体应在 DSE 生命周期全过程实施符合相关法规、标准的管理，组织 DSE 相关活动等。

6.2 管理主体

应首先明确评价工作机构的管理主体，并在管理主体的支持、指导下开展DSE相关活动。管理主体的职责主要应包括：

a) 理解数据（个人信息）安全，明确 DSE 的目的；
b) 提供利于 DSE 的管理平台，积极推进 DSE；

c) 组建相应的工作机构，遴选具有相应知识、能力、专业等的管理人员，保证 DSE 的实施；
d) 为推进、实施 DSE 提供所需资源支持，包括人员、资金、信息、管理、环境等；
e) 对 DSE 管理过程中可能出现的各种不利因素提供管理决策；
f) 对 DSE 管理和 DSE 提供指导和决策；
g) 批准 DSE 工作机构的组建、职责分配及相应的管理机制等。

6.3 工作机构

6.3.1 要求

管理主体应依据DB21/T XXXX.1 4.2指导、批准设立DSE工作机构：
a) 依据 DB21/T XXXX.1 4.2.2，工作机构名称宜称为数据安全工作委员会；
b) 依据 DB21/T XXXX.1 4.2.2.1，工作机构的构成应具有广泛的代表性，不应局限于某一领域或行业；
c) 依据 DB21/T XXXX.1 4.2.2.1，工作机构应根据 DSE 的特征和功能属性，设立若干职能单元，分工负责，共同履行工作机构的职能。

6.3.2 管理

工作机构应依据DB21/T XXXX.1 4.2.2，建立相应的管理机制：
a) 应明确管理章程，确定工作机构的目标；
b) 应依据管理章程建立相应的工作机制、管理流程；
c) 应明确各项职能，参看 DB21/T XXXX.1 4.2.2.2；
d) 应明确工作机构成员的产生机制、工作职责等。

6.3.3 职能单元

依据DB21/T XXXX.1 4.2.2.1，工作机构宜设立若干职能单元，宜包括：
a) 法规组：法规组的职能应包括：
   1) 数据（个人信息）安全相关法规、标准、制度的研制；
   2) 数据（个人信息）安全相关法规、标准、制度的相关理论和实践研究、解释；
   3) DSE 相关规则、标准研制、审核；
   4) DSE 相关规则、标准的相关理论和实践研究、解释；
   5) DSMS（PISMS）建设咨询、指导等；
b) 仲裁组：仲裁组的职能应包括：
   1) 数据（个人信息）安全事件、事故的认定、说明；
   2) 数据（个人信息）安全事件、事故的处理、说明；
   3) 数据（个人信息）管理与数据（个人信息）主体之间的问题处理、说明；
   4) DSE 相关投诉、质疑的处理、说明；
   5) 数据（个人信息）安全相关问题咨询、指导等；
c) 宣传组：宣传组的职能应包括：
   1) 理解、阐释数据（个人信息）安全相关法规、标准；
   2) 理解、阐释 DSE 相关规则、标准；
   3) 数据（个人信息）安全相关法规、标准、制度的宣贯、推广；
   4) DSE 相关规则、标准的宣贯、推广；
   5) 数据（个人信息）安全相关知识、实践的阐述、说明；

6) DSMS（PISMS）相关知识、实践的阐述、说明
7) DSE 相关知识、实践的阐述、说明；
8) 数据（个人信息）管理相关问题咨询、说明等；

d) 国际交流组：国际交流组的职能应包括：
1) 数据（个人信息）安全相关法规、标准、制度的解释、说明；
2) DSE 相关规则、标准的解释、说明；
3) 数据（个人信息）安全相关法规、标准、制度的相关理论和实践研究的说明；
4) DSE 相关规则、标准的相关理论和实践研究说明；
5) 国际间的交流、合作；
6) 中国数据（个人信息）安全相关问题的咨询、解释、说明等；

e) 教育培训组：教育培训组的职能应包括：
1) 面向社会：
- 数据（个人信息）安全基础理论、实践教育、培训；
- 数据（个人信息）安全相关法规、标准、制度的解读、培训；
- DSE相关规则、标准的解读、培训；
- DSMS（PISMS）实训教育、培训等；

2) 面向内部：
- 数据（个人信息）安全基本知识；
- DSE基本知识；
- 数据（个人信息）安全相关法规、标准、制度；
- DSE基本知识、规则、标准；
- DSMS(PISMS)实训；
- 评价人员基本技能；
- 评价人员基本素质等。

6.4 评价机构

6.4.1 要求

依据DB21/T XXXX.1 4.2.3，评价机构应是管理机构为管理、实施DSE派出的评价主体：

a) 依据 DB21/T XXXX.1 4.2.3，评价机构的组成应具有权威性、代表性；
b) 依据 DB21/T XXXX2.1 4.2.3，评价机构应设立常设机构，处理日常事务、管理评价相关事宜等。

6.4.2 职能单元

评价机构的职能，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） 组织现场审核；
5） 提交 DSE 相关文档；
6） DSE 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） 培训教育效果评估等；

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 相关文档的管理等；

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 相关事务等。

6.5 职责

评价机构应明确管理职责，主要应包括：

a） DSE 的前期咨询、解释；
b） 数据（个人信息）安全相关法规、标准的解释、说明；

c） DSE 相关规则、标准的解释、说明；
d） DSMS（PISMS）建设指导、咨询；
e） 受理 DSE 申请；
f） 审查 DSE 申请资格；
g） 评价人员聘用、管理；
h） DSE 现场审核组组建、管理；
i） DSE 相关文档管理；
j） 评价结论、评价资格管理；
k） 投诉、建议和反馈管理等。

6.6 管理

6.6.1 要求

评价机构应依据DB21/T XXXX.1 4.2.3，建立相应的管理机制：
a） 应建立评价机构管理制度和相应的实施细则；
b） 应建立评价机构工作流程、评价管理机制；
c） 应明确评价机构各项管理职能；
d） 应明确评价管理人员的职责和义务等。

6.6.2 管理制度

应建立评价机构管理的相关规章制度，主要应包括：
a） 评价机构的构成和职责；
b） 评价机构服务准则；
c） 评价机构工作流程；
d） 评价事务管理；
e） 安全保密规定；
f） 相关文档管理；
g） 罚则；
h） 其它必要的制度等。

6.7 工作流程

评价机构应建立工作流程，如图1示。

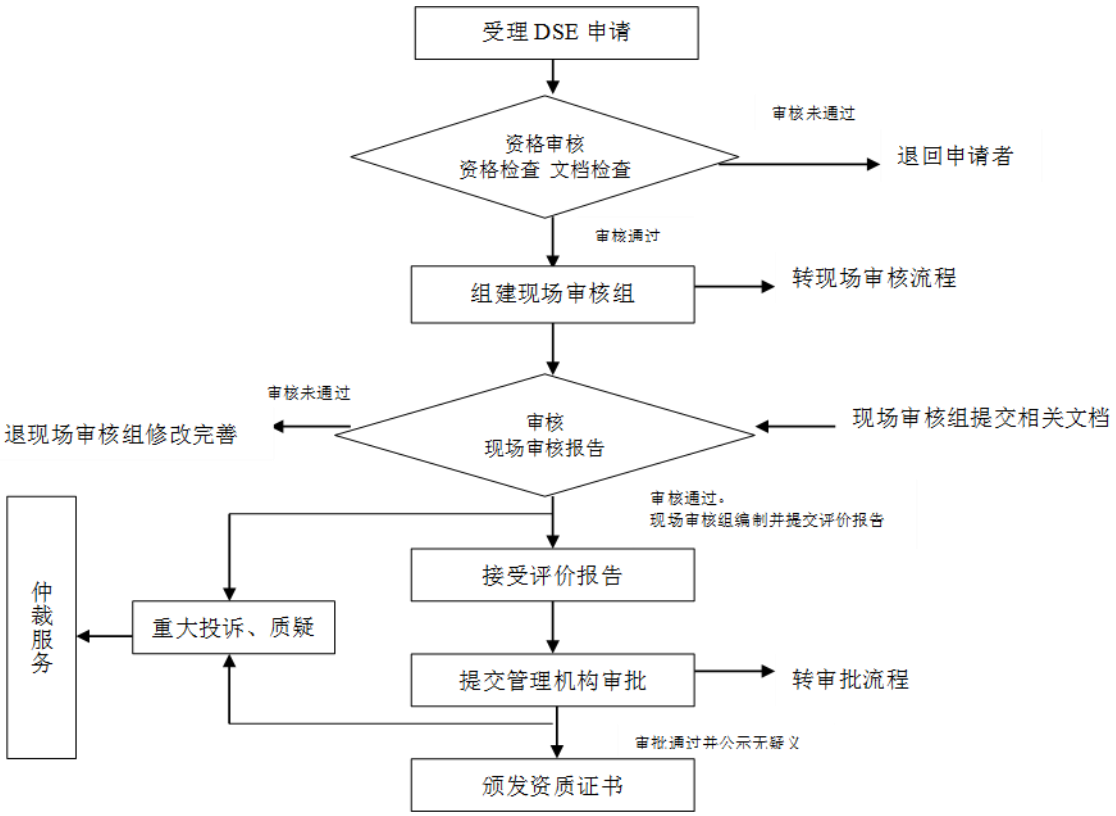

图1　评价机构工作流程

7　评价管理

7.1　概述

7.1.1　要求

DB21/T XXXX.1第4章确立了DSE的基本规则，评价主体应符合DB21/T XXXX.1 4.2.3的规定，并应基于DB21/T 1628、DB21/T XXXX系列标准，依据DB21/T XXXX.1和本文件实施DSE。

7.1.2　原则

评价主体应遵循DB21/T XXXX.1 4.1确立的DSE的基本原则，并在评价中细化、明确原则实施的细节，保证DSE的客观性、有效性和充分性。

7.2　评价边界

依据DB21/T XXXX.1，评价主体应确定DSE的边界，主要应包括：

a)　范围和特征：个人信息的分布范围和存在特征；
b)　层级和权责：个人信息管理者内部管理、业务层次和权限、责任及与 DSMS（PISMS）的关系；
c)　部门间：数据（个人信息）管理者内部各部门之间的关联、影响及与 DSMS（PISMS）的关系；
d)　外部：数据（个人信息）管理者与客户、社会组织之间的关联、影响及对 DSMS（PISMS）的影响；
e)　责任主体：与数据（个人信息）相关责任主体的职能、职责、权限；

f） 体系设计：DSMS（PISMS）的层级及权责设计；
g） 业务关系：DSMS（PISMS）与业务连续性的关系；
h） 变化：数据（个人信息）管理者内部管理、业务发生变化对 DSMS（PISMS）的影响；
i） 个人：数据（个人信息）管理者的员工、DSMS（PISMS）相关人员的行为、责任等。

7.3 组织

评价机构应依据数据（个人信息）安全相关法规、标准，组织DSE相关活动：
a） 建立 DSE 体系，保证 DSE 的质量；
b） 明确评价管理职责和管理人员行为规范；
c） 选择、聘请具有相应能力的评价人员，保证评价的独立性、客观性；
d） 实施 DSE；
e） 评估 DSE 质量、效果；
f） DSE 后管理；
g） 其它相关管理等。

7.4 控制

评价机构应依据数据（个人信息）安全相关法规、标准，检查、修正评价管理相关活动，监督、跟踪DSE的实施。

7.5 协调

评价机构在评价管理中，应注意与第一方、评价人员、现场审核组、管理机构等之间的协调、沟通：
a） DSE 目的的一致性、实施有效性；
b） DSE 边界的合理性、特征符合性；
c） 评价人员的能力、水平和公正性、客观性；
d） 评价方法、手段的适宜性、可用性；
e） 评价指标的符合性、适用性；
f） 评价流程的可用性；
g） 评价质量的可控性；
h） 评价结果的准确性、客观性、科学性等。

8 评价体系

8.1 评价要素

DSE的要素，主要应包括：
a） 评价目的：DSE 应实现的目标；
b） 评价主体：评价机构；
c） 评价对象：DSMS（PISMS）；
d） 评价因素：DSE 指标体系、指标因子；
e） 评价方法：DSE 规则、各种方法；
f） 等级：DSE 等级标准和划分原则；
g） 权重：DSE 指标的影响度、重要性；
h） 评价过程：DSE 过程管理；

i） 评价结果：获得 DSE 的结果；
j） 评价效益：评价主体的主客观因素对评价结果的影响和认可等。

8.2 评价规则

DSE的规则，主要应包括：
a） 确定 DSE 指标；
b） 根据数据（个人信息）安全相关法规、标准制定评价等级标准；
c） 根据等级标准划分评价等级和每个等级的评分范围；
d） 确定评价指标子项和对应的分值；
e） 根据等级标准对各个评价指标和指标子项评分、加权，计算得分和总分等。

8.3 评价等级

应根据数据（个人信息）安全相关法规、标准划分评价等级，以区分数据（个人信息）安全程度。评价等级可划分为4级：
a） 1 级：在基于数据（个人信息）生命周期全过程的管理中，存在明显的缺陷，DSMS（PISMS）不完善，评价总分较低；
b） 2 级：在基于数据（个人信息）生命周期全过程的管理中，存在部分缺陷，但 DSMS（PISMS）较完善，评价总分一般；
c） 3 级：在基于数据（个人信息）生命周期全过程的管理中，存在微小缺陷，DSMS（PISMS）完善，评价总分较高；
d） 未通过现场审核：在基于数据（个人信息）生命周期全过程的管理中，存在严重缺陷，不能保证数据（个人信息）安全和数据（个人信息）主体权益等。

8.4 评分范围

评价总分应采用百分制，并确定DB21/T XXXX.1 8.3规范的评价等级的取值空间，一般可划分为：
a） 1 级：评分范围可在 25 分内，如 50-75；
b） 2 级：评分范围可在 15 分内，如 75-90；
c） 3 级：评分范围可在 10 分内，如 90-100。

8.5 构建 DSE 体系

评价机构应依据DB21/T XXXX.1 4.3组织构建评价体系：
a） 明确 DSE 的目的，确立 DSE 的基本原则；
b） 确定评价对象，根据评价对象的特征，明确 DSE 的边界和 DSE 的相应资源需求；
c） 建立评价机构的管理机制，明确机构职能、管理职责和相关人员的职责；
d） 选聘具有相应能力的评价人员，建立相应的评价人员管理机制、培训机制和能力评价机制；
e） 基于评价对象的特征，分析、判断评价对象的各种关联因素，选择适宜的评价方法和手段；
f） 基于评价对象的特征，设计、建立相应的 DSE 指标体系；
g） 基于数据（个人信息）管理者的实际和评价规则，确定评价指标的权重；
h） 建立科学、规范的评价流程，包括受理申请、资格审核、现场审核、仲裁服务、审批、资格管理等；
i） 建立 PDCA 过程管理模式，在 DSE 实施中，不断修正、改进评价流程，持续改进评价体系；
j） 建立评价质量管理体系，通过过程管理，跟踪、监控评价过程；
k） 建立评价结果管理机制，保证评价数据、信息可靠，判断、评估科学、客观。

9 评价指标

9.1 概述

9.1.1 要求

依据DB21/T XXXX.1 5.1，评价机构组建现场审核组后，应由现场审核组根据数据（个人信息）管理者的特征，设计并建立DSE指标体系。

9.1.2 指标体系

指标体系应考虑的要素，主要应包括：

a) 数据（个人信息）安全相关法规、标准；
b) 数据（个人信息）安全目标和 DSE 目的；
c) 数据（个人信息）管理者的组织、管理、业务特征；
d) 数据（个人信息）管理者的环境（包括工作环境）特征；
e) 数据（个人信息）管理者内部个人信息的分布、关联因素；
f) 数据（个人信息）管理活动、行为和变化；
g) DSMS（PISMS）的构建、实施和运行；
h) DSMS（PISMS）内审内容设计和内审结果；
i) 资格审核中文档审查结果；
j) 数据（个人信息）管理者与外部的关联和影响等。

9.2 设计

依据DB21/T XXXX.1 5.2，DSE指标设计应考虑多种因素间的关联关系：

a) 整体评价与评价指标：各个评价指标的评估、判断，应是相互关联的，形成 DSMS（PISMS）的整体评价；
b) 评价指标间：应在设计评价指标时，考虑评价指标之间、评价指标项之间相互关联的整体关系，避免雷同、重复、矛盾和混乱，降低复杂度和评价成本；
c) 评价指标项间：应考虑单一指标项的合理性与整体评价中各个指标项的合理性；
d) 业务流程与评价指标：应考虑评价指标的客观、全面、系统与业务流程的自由度；
e) 管理与执行：应综合判断、评估个人信息管理者内部管理层、执行层等各层级的个人信息管理状况；
f) DSMS（PISMS）：应全面、整体评估、判断 DSMS（PISMS）、体系内各个功能要素之间的关联关系；
g) 评价指标与评价结果：应考虑评价指标与评价结果之间可供选择的评判区间，整体、全面、综合评价 DSMS（PISMS）等。

9.3 评估

应依据DB21/T XXXX.1 5.3，评估DSE指标体系的科学性、合理性、可用性和有效性，完善并持续改进：

a) 指标体系与数据（个人信息）安全相关法规、标准的符合性；
b) 指标体系与数据（个人信息）管理者实际的符合性；
c) 评价指标、指标项的合理性、针对性；
d) 评价结果与评价指标间的契合度等。

10 过程管理

10.1 要求

DSE应依据DB21/T XXXX.1 第7章、第8章和第9章的规则，遵循DB21/T XXXX.1 第6章确立的流程实施。

10.2 管理机制

DSE过程中，应明确相关管理机制：

a) 确定 DSE 的目标、方法、策略；
b) 确定清晰的质量管理目标；
c) 明确管理机构、管理人员和评价人员的职责；
d) 保证资格审核、现场审核的独立性、公正性和权威性；
e) 保证评价人员的业务素养、个人修养、专业水平；
f) 确定以评价对象为中心、基于事实管理的原则；
g) 保证 DSE 相关文档的严谨、规范、完整；
h) 建立 DSE 追踪、评估机制；
i) 建立投诉仲裁、意见反馈机制；
j) 其它必要的管理机制等。

10.3 评价机构

评价机构应依据评价工作流程：

a) 评价机构的常设机构应依据 DB21/T XXXX.1 8.1.2 审查 DSE 申请者的资格，确认 DSE 申请者具有 DSE 申请资格；
b) 确认 DSE 申请者具有 DSE 申请资格后，选聘具有相应能力的评价人员，审查 DSE 申请者提交的 DSE 申报文档等。

10.4 评价实施

10.4.1 资格审核

10.4.1.1 资格审查

依据DB21/T XXXX.1 8.1.2 确立的资格审查内容，评价机构的常设机构应审查DSE申请者的申请条件、提交的DSE相关文档，并作出审查结论。

10.4.1.2 审查方式

资格审查方式主要可包括面谈、文档检查等。

10.4.2 文档审查

评价机构选聘的评价人员，应依据DB21/T XXXX.1 8.1.3 确立的资格审查规则和内容，审查DSE申请者提交申报文档，初步评估DSE申请者个人信息管理的有效性和法规、标准的符合性，明确需要整改的问题和需要现场审核确认的问题，并提出审查意见。

10.4.3 整改报告

在资格审查、文档审查中确认需要整改的问题，均应形成整改意见，反馈到DSE申请者；DSE申请者应在整改完成后提交整改报告，说明整改措施等。

10.4.4 审核结论

审查文档的评价人员，应依据DB21/T XXXX.1 8.2、资格审查结论、文档审查意见、整改报告，形成资格审核结论，并依据DB21/T XXXX.1 8.3编制资格审核报告。

10.4.5 现场审核

10.4.5.1 要求

资格审核确认后，评价机构应依据DB21/T XXXX.1 第9章，组建现场审核组，实施现场审核：

a) 审核组宜由负责文档审查的评价人员担任组长；
b) 审核组应根据 DB21/T XXXX.1 第 11 章的规则选聘适宜的现场审核评价人员等。

10.4.5.2 审核过程

现场审核组应依据DB21/T XXXX.1第9章，展开现场审核。

10.4.5.3 审核结论

应依据DB21/T XXXX.1 9.5形成审核结论：

a) 应累积、整理、分析现场审核过程中的所有信息；
b) 应根据分析结果和资格审核报告判断、评估 DSMS（PISMS）；
c) 根据 DB21/T XXXX.1 9.5.2 确立的问题分类原则和 DSMS（PISMS）评估结果，明确说明存在的问题和解决建议；
d) 形成公正的审核结论等。

10.4.5.4 审核意见

应依据DB21/T XXXX.1 9.5.3形成审核意见。

10.4.5.5 整改

现场审核等级确定为1级、2级，应依据DB21/T XXXX.1 9.6整改，并提交整改报告。现场审核组应评估接受现场审核的数据（个人信息）管理者提交的整改报告，并提出相应的意见。

10.4.5.6 现场审核报告

现场审核结束后，应依据DB21/T XXXX.1 9.7形成现场审核报告。

10.4.6 报告审核

评价机构应依据DB21/T XXXX.1 10.1审核现场审核组提交的DSE相关文档。

10.4.7 评价报告

评价机构审核通过后，现场审核组应依据DB21/T XXXX.1 10.2编制PISMSE报告。

10.5 审批和公示

管理机构应依据DB21/T XXXX.1 10.3审批评价报告。并应在审批通过后，依据DB21/T XXXX.1 10.4，采取适当方式公示。

10.6 仲裁服务

如DSE申请者对DSE过程存在异议、疑义等，可申请仲裁服务。

11 人员管理

应依据DB21/T XXXX第12章，建立DSE人员的管理机制。

12 文档管理

应依据DB21/T XXXX.1 第13章的规则，建立、完善DSE所有相关文档的管理。

13 过程改进

应建立、完善DSE过程改进、完善机制：

a) 应依据 DB21/T XXXX.1 第 14 章确立的规则实施过程改进；
b) 应参照 DB21/T 1628.2 第 14 章和 DB21/T 1628.8 的过程管理方法，不断改进、完善 DSE 体系。

14 资格管理

应遵循DB21/T XXXX.1第15章的规则，建立、完善取得DSE资格后的管理机制。