ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX.5—XXXX

信息安全技术 数据安全评价 第5部分：评价方法

Information Security technology-data security evaluation part5：evaluation methodology

（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

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5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5部分：评价方法

1 范围

本文件规定了数据安全评价的软评价、综合评分方法、现场审核方法、兼容性和改进等规则。

本文件适用于各类数据安全评价机构，亦为已建立数据（个人信息）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 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

DB21/T XXXX.2 信息安全技术 数据安全评价 第2部分：管理指南

3 术语和定义

DB21/T XXXX、DB21/T XXXX、 DB21/T XXXX.1界定的术语和定义适用于本文件。

4 要求

本文件遵循DB21/T XXXX.1确立的DSE的基本原则和要求，重点描述和规范DSMS（PISMS）评价方法。

DSMS（PISMS）评价方法，应以DB21/T 1628系列标准、DB21/T XXXX为基准。

DSMS（PISMS）评价方法，应同时使用DB21/T XXXX.1和本文件，并参照DB21/T XXXX系列其它标准。

DSMS（PISMS）评价方法，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的认证方法。

5 软评价

5.1 概述

DSE，数据（个人信息）管理者数据（个人信息）管理状况的相关信息采集、分析、判断、评估过程。在这个过程中，更多基于主观判断，定性分析、评估。因而，DSE一般应采用软评价方法。

软评价方法，即利用知识、专业、经验等，依据数据（个人信息）安全法规、标准，判断、评估数据（个人信息）管理者的数据（个人信息）管理质量，准确评价数据（个人信息）的安全性。

5.2 相关因素

软评价的相关因素，主要应包括：

a) 数据（个人信息）管理者：
   1) 申请 DSE 基本信息；
   2) 资格审核信息；
   3) DSMS（PISMS）运行报告；
   4) 安全风险评估；
   5) 现场审核信息等；
b) 审核员：
   1) 专业水平：综合知识能力；
   2) 技术能力：专业、知识应用能力；
   3) 业务素养：经验和解决问题的能力；
   4) 个人修养：自身素质、职业道德、沟通交际能力等；
   5) 团队意识：审核组内部的协商、沟通、处理问题能力等。

5.3 标准方法

DSE采用的标准方法，主要应包括：

a) 国家法律：数据安全法、个人信息安全法；
b) 国家标准：GB/T 35273-2020 《信息安全技术 个人信息安全规范》；
c) 地方标准：DB21/T 1628 系列、DB21/TXXXX、DB21/T XXXX 系列。

5.4 非标准方法

DSE采用的非标准方法，主要应包括：

a) 评价机构自定义的相关评价规则；
b) 资格审核方法；
c) 现场审核方法；
d) 数据（个人信息）管理者定义的规章制度等。

6 综合评分方法

6.1 信息收集

6.1.1 资格审核

评价机构接受DSE申请后，应有针对性的收集DSE申请者的相关信息：

a) 通过面谈、文档收集 DSE 申请者的基本信息；
b) 通过面谈、网站等多种方式收集 DSE 申请者的相关信息；
c) 通过资格审查、文档审查收集 DSE 申请者的细节信息等。

6.1.2 现场审核

现场审核组在现场审核过程中，应有目的、有计划的依据评价指标收集DSE申请者的现场相关信息：

a) 通过会议、介绍说明等收集现场基本信息；
b) 通过会议、数据（个人信息）管理说明等收集 DSMS（PISMS）基本信息，

c） 通过走访、调研等收集现场细节信息；
d） 通过与 DSE 申请者内部员工面谈等收集相关信息；
e） 通过文档收集相关信息等。

6.1.3 评价审核

评价机构接受资格审核报告、现场审核报告后，应与审核组、审核员沟通，获取报告相关信息。

6.2 综合分析

6.2.1 资格审核

审核员应通过梳理获得的信息，综合分析DSE申请者的申请资格，并提出审核意见：
a） 与 DSE 申请者之间的疑义交流、沟通；
b） 评价机构内部的沟通、讨论；
c） 与相关人士的沟通等。

6.2.2 现场审核

现场审核组应通过整理、梳理现场获得的信息，综合分析DSE申请者的现场审核情况，并提出审核意见：
a） 审核员独立分析、评判、评分；
b） 审核员互相交流，可修正评分；
c） 会议讨论，交流评分偏差；
d） 与资格审核信息比对；
e） 与 DSE 申请者疑义交流；
f） 与 DSE 申请者关联关系交流；
g） 确定评分结果等。

6.2.3 评价审核

评价机构应整合资格审核报告、现场审核报告、审核组、审核员等获取的信息，综合分析、评判，并提出评价机构对审核结论的审核意见。

7 专家评判方法

7.1 过程评判

DSE过程中，审核组可聘请管理机构、评价机构及其它相关专业人士，探讨、研究DSE过程中的无法确认的问题：
a） 可独立思考、打分，形成各自的意见；
b） 可集中讨论、分析意见差异、异议；
c） 形成统一的意见；
d） 难以统一的认知可形成特定的案例；
e） 具有典型意义的问题可形成案例等。

7.2 评审审批

评价机构审核通过后，应向工作机构提交评价报告，由工作机构组织专业人士、相关专家等审批：

a) 听取审核组报告，获取 DSE 相关信息；
b) 提出质疑，疑义、异议；
c) 综合分析审批会议获得的信息，获得独立认知；
d) 形成各自独立的意见；
e) 形成审批意见等。

7.3 案例讨论

对特定案例、典型意义案例，应组织相关专业人士、相关人员研讨：
a) 案例当事人应详细说明案例的相关信息；
b) 提出各自不同的案例认知；
c) 归纳、总结；
d) 形成基本一致的意见；
e) 仍然不能解决的问题可提交工作机构，形成研究课题等。

8 现场审核方法

8.1 审核会议

8.1.1 要求

现场审核组应依据DB21/T XXXX.1第9章确立的规则，召开现场会议，宣传数据（个人信息）相关法规、标准，说明DSE目的、计划、方法、过程等。

8.1.2 审核准备

现场审核组进入审核现场前，应召开准备会议。会议主要内容应包括：
a) 明确 DSE 的目的、任务；
b) 沟通，了解、熟悉数据（个人信息）管理者的基本情况、业务范围等；
c) 了解资格审核报告内容及 DSMS（PISMS）构建、实施、运行状况；
d) 部署现场审核计划、审核时间、阶段和进度，以及审核员的分工范围；
e) 说明评价指标设计；
f) 现场审核的质量保证措施；
g) 审核员的相关专业知识培训、讲解等。

8.1.3 进入现场

现场审核组进入审核现场，应召开工作会议：
a) DB21/T XXXX.1 第 9 章确定的主要会议内容及其它必要事项；
b) 形成对数据（个人信息）管理者的初步、整体的基本认识；
c) 形成对 DSMS（PISMS）运行状况的基本了解；
d) 与数据（个人信息）管理相关人员建立信任、合作的基础；
e) 建立审核双方认可的信息安全承诺等。

8.1.4 审核过程

现场审核组在审核过程中，应依据DB21/T XXXX.1 第9章适时召开工作例会：
a) DB21/T XXXX.1 第 9 章确定的主要会议内容及其它必要事项；

b) 检查审核方法、样本选择；
c) 检讨审核过程中可能存在的问题；
d) 需要再次评估的问题；
e) 需要与数据（个人信息）管理相关人员沟通、协调的问题；
f) 形成一致、统一的意见等。

8.1.5 审核结束

现场审核组结束现场审核后，应依据DB21/T XXXX.1 第9章召开工作会议：
a) DB21/TXXXX.1 第 9 章确定的主要会议内容及其它必要事项；
b) 现场审核意见定性、定量描述、说明；
c) 听取数据（个人信息）管理者相关人员的解释和说明；
d) 与数据（个人信息）管理者达成共识；
e) 形成统一的结论等。

8.2 调查方式

8.2.1 计划调查

审核员应根据审核计划分工，按照评价指标项独立展开调查，并形成调查意见：
a) 审核员应了解数据（个人信息）管理者的基本情况；
b) 审核员应明确分工部分的调查对象、调查内容、调查目标等；
c) 审核员应选择适宜的调查方法等。

8.2.2 意见综合

审核组组长应适时召开审核会议，综合审核员的调查意见：
a) 审核员提交各自的调查意见；
b) 无疑义的调查意见应形成统一的审核意见；
c) 提取调查意见的分歧点，提交会议讨论，并形成统一的意见等。

8.3 调查方法

8.3.1 要求

现场审核组在审核过程中，应依据DB21/T XXXX.1 9.3展开现场调查：
a) 应通过现场调查获取真实的 DSE 原始数据；
b) 应比较现场获取数据与申报数据的符合性、一致性和有效性；
c) 应通过文档检查确认申报文档的完整性、真实性；
d) 应充分了解数据（个人信息）管理者，根据实际、申报文档等设计面谈大纲和内容；
e) 面谈可在审核过程中的任一阶段，根据调查需要实施等。

8.3.2 面谈

8.3.2.1 面谈方式

应依据面谈大纲分别访问相关人员。面谈方式可包括：
a) 集体面谈：与 DSMS（PISMS）相关责任人集体访谈，调查并确认 DSMS（PISMS）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（个人信息）安全的理解和DSMS（PISMS）对个人的影响；
c) 客户面谈：宜与个人信息管理者的相关客户接触，调查客户对个人信息管理状况的认知和DSMS（PISMS）对客户的影响等。

8.3.2.2 面谈样本

现场审核人员应根据现场审核准备阶段确定的审核目标、审核内容及资格审核中需要确认的问题，设计面谈样本。面谈样本的选择：

a) 集体面谈，样本选择应包括：
   1) 最高主管领导；
   2) DSMS（PISMS）所有相关责任主体；
   3) 也可根据需要选择关键部门责任主体等；
b) 个人面谈，样本选择应包括：
   1) 最高管理者（可根据实际情况选择）；
   2) DSMS（PISMS）相关责任主体；
   3) 关键部门员工；
   4) 可根据实际需要随机选择其它员工等。

8.3.3 文档检查

审核组应参照DB21/T1628.2、DB21/T 1628.4，检查相关文档，调查并确认数据（个人信息）管理机制的状况：

a) 数据（个人信息）管理相关文档，包括管理计划及相关原始记录和资料等；
b) DSMS（PISMS）相关文档，包括责任主体及职能职责、规章制度、宣传教育、过程管理等，及相关的原始纪录和资料；
c) 个人信息数据库，包括个人信息的分布、组织结构、管理机制及相关原始记录和资料；
d) 信息安全相关文档和资料等。

8.3.4 业务抽查

8.3.4.1 要求

应在现场审核中，根据需要抽查数据（个人信息）相关业务。应选取适宜的抽查样本，调查DSMS（PISMS）实施、运行状况：

a) 根据审核计划、数据（个人信息）管理者实际确定抽查样本；
b) 根据面谈、文档检查确定抽查样本等。

8.3.4.2 样本选择

8.3.4.2.1 要求

业务抽查样本选择，应基于以下准备：

a) 了解数据（个人信息）管理者的基本情况；
b) DSE资格审核；
c) 面谈、文档审查等。

8.3.4.2.2 样本

应依据DB21/T XXXX.1确定的规则和其它可能的情况，选择适当的调查样本。一般考虑：

a) 业务流程：应选择典型的、与数据（个人信息）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（个人信息）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（个人信息）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。

8.3.4.3 抽样范围

选取抽查样本的范围，一般应考虑：

a) 包括时间范围、样本选择范围、样本检查范围等：
   1) 时间范围：DSMS（PISMS）构建、实施和运行的时间节点；
   2) 样本选择范围：根据 DB21/T XXXX.1 确定样本覆盖的范围；
   3) 样本检查范围：根据样本选择范围确定样本检查节点等；
b) 依据数据（个人信息）安全相关法规和标准、DSMS（PISMS）现场审核计划和数据（个人信息）管理者的实际，以及 DSMS（PISMS）实施、运行状况确定；
c) 抽查范围应根据现场审核情况随时调整等。

8.3.4.4 抽样数量

8.3.4.4.1 规则

抽样数量应保证抽查样本可以反映数据（个人信息）管理的总体特征，并相对准确，以提高现场审核效率：

a) 总体特征：数据（个人信息）管理者内部数据（个人信息）的分布、业务特征、管理特征及各种关联关系等；
b) 准确率：保证各个抽查样本覆盖数据（个人信息）管理的总体特征，不应单纯追求数量；
c) 层次化：可在抽查范围内，划分评价对象的不同层次，重点层次可适当多的选取抽查样本等。

8.3.4.4.2 要求

确定抽样数量，一般应考虑：

a) 规模：抽样数量可根据数据（个人信息）管理者的规模确定；
b) 实际状况：应根据数据（个人信息）管理的重视程度、DSMS（PISMS）实施运行的有效性确定；
c) 关键业务单元：涉及数据（个人信息）的关键业务单元的可信性、安全性；
d) 缺陷：应根据数据（个人信息）管理和 DSMS（PISMS）实施运行的缺陷和薄弱环节确定等。

8.3.4.5 抽查结论

抽样调查结束后，应基于面谈、文档审查和抽查过程，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（个人信息）安全相关法规、标准形成等。

注：多种调查方法应结合使用。

9 兼容性

如数据（个人信息）管理者已经通过信息安全管理体系认证，在确定DSE方法时，应综合、系统考虑信息安全管理体系认证与DSE的兼容性。

10 改进

应随时评估评价方法的合理性、适用性和方法风险，并不断改进、完善。