ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX.8—XXXX

信息安全技术 数据安全评价 第8部分：保证方法

Information Security technology-data security evaluation part8：assurance methods

（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8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8部分：保证方法

1 范围

本文件规定了数据安全评价保证方法参考图示、偏差处理、质量管理等相关要求。

本文件适用于为数据安全评价中偏差处理、质量管理提供指导规则。

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8部分：过程管理

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.3 信息安全技术 数据安全评价 第3部分：审核员管理

DB21/T XXXX.4 信息安全技术 数据安全评价 第4部分：评价指标

DB21/T XXXX.6 信息安全技术 数据安全评价 第6部分：资格审核

DB21/T XXXX.7 信息安全技术 数据安全评价 第7部分：现场管理

DB21/T XXXX.10 信息安全技术 数据安全评价 第10部分：审批管理

3 术语和定义

GB/T 19001/ISO 9001、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，重点描述和指导DSE的质量保证。

DSE保证方法，应以DB21/T 1628系列标准、DB21/T XXXX为基准。

DSE质量保证，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。

DSE质量保证，亦应同时参考信息安全、质量管理、服务管理等其它标准体系。

5 综述

保证方法，是数据（个人信息）安全管理体系评价的质量保证。评价机构应制定有效保证数据（个人信息）安全管理体系评价质量的计划、方法、策略，在标准实施、评价流程、实践方法中正确采用。

数据（个人信息）安全管理体系评价质量的保证方法，主要应包括资格审核（DB21/T XXXX.6）和现场审核（DB21/T XXXX.7）的偏差处理和质量控制。

6 参考图示

保证方法的参考图示，如图1示。

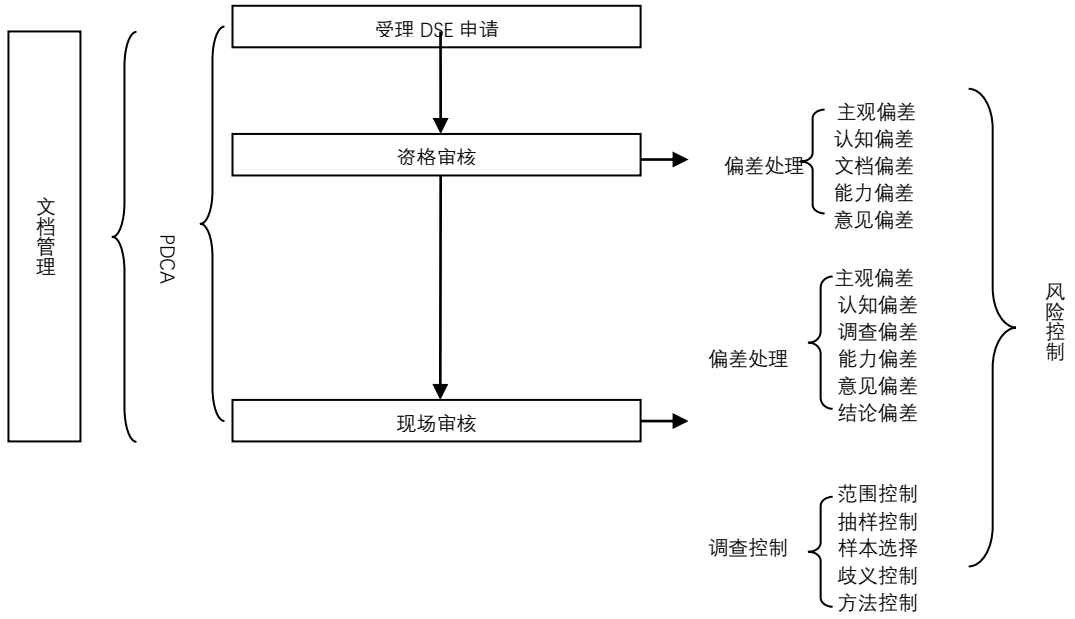

图1 保证方法参考图示

7 偏差处理

7.1 综述

在DSE中，偏差是影响评价质量的重要因素，DSE偏差可能是多方面的，应在DSE过程中修正、调节。

7.2 认知

7.2.1 偏差源

在DSE中，偏差可存在于资格审核和现场审核中：

a) 资格审核中可存在的偏差，如：
   1) 主观偏差；
   2) 认知偏差；
   3) 文档偏差；
   4) 能力偏差；
   5) 意见偏差等；
b) 现场审核中可存在的偏差，如：
   1) 主观偏差；
   2) 认知偏差；
   3) 调查偏差；
   4) 能力偏差；
   5) 意见偏差；

6） 结论偏差等。

7.2.2 原因

在DSE中，产生偏差的原因，可存在于：

a） 资格审核、现场审核的倾向性；
b） 专业、知识能力欠缺；
c） 业务能力差异；
d） 争议处理；
e） 与 DSE 申请者之间的利益相关性；
f） 审核结论的偏见、倾向性等。

7.2.3 识别

偏差应在DSE过程中识别：

a） 评价机构应在资格审核、组建现场审核组、现场审核管控、报告审核和审批过程中识别可能的偏差；
b） 现场审核组应在现场审核中识别可能的偏差；
c） DSE 结束后应回溯 DSE 过程，识别潜在的偏差等。

7.3 分类

在DSE过程中，产生偏差的影响程度不同，划分偏差等级不同：

a） 轻偏差：非实质性偏差，不影响 DSE 质量，如：
   1） 文档记录不规范、不完整；
   2） 缺少确认签字等；
b） 一般偏差：可对 DSE 质量产生实际或潜在影响，如：
   1） 忽略资格审核中需现场审核确认的问题；
   2） 抽样调查中样本选择有误；
   3） 现场调查中忽视实质问题；
   4） 审核结论存在争议等；
c） 严重偏差：可对 DSE 质量、DSE 结论的权威性、公正性产生重大影响和后果，如：
   1） 专业、知识能力欠缺使 DSE 缺失专业性、规范性；
   2） 审核过程、审核结论的倾向性；
   3） 存在利益相关性等。

7.4 处理

7.4.1 培训教育

评价机构应依据DB21/T XXXX.3定期组织评价人员培训教育：

a） DB21/T XXXX.3 第 6 章规定的职业规范教育；
b） 依据 DB21/T XXXX.3 第 8 章的规定培训各级别评价人员的能力。

7.4.2 资格审核

评价机构应依据DB21/T XXXX.3第10章定期、年度审核评价人员评价资格。

7.4.3 过程管理

在DSE过程中，应随时纠正显见的、可识别的潜在偏差：

a) 初步评估：在 DSE 过程中，如识别出显见的、可识别的潜在偏差：
   1) 应报告审核组长，采取控制措施；
   2) 应依据本文件分析、评估偏差的原因；
   3) 应评估偏差的影响和结果等；
b) 类型评估：现场审核组应依据本文件并根据初步评估结果分析、判断、评估偏差的类型，确定偏差对 DSE 的影响；
c) 修正措施：根据不同类型的偏差采取相应的修正措施：
   1) 轻偏差：DSE 现场即行纠正；
   2) 非轻偏差：应根据评估结果确定修正措施：
      - 严格规范DSE流程，重新实施现场审核；
      - 审核人员现场补充知识能力；
      - 现场更换审核员（如有可能）；
      - 停止DSE现场审核等。

注1：应在修正偏差后评估纠正措施的有效性。

7.4.4 追溯管理

评价机构应监督现场审核组追溯DSE过程，发现DSE过程中未识别的潜在偏差：

a) DSE 结束后的评价过程评估；
b) 定期梳理、总结 DSE 案例；
c) 典型案例整理等。

发现偏差，应参照7.4.3的规定评估偏差：

a) 轻偏差：可追溯纠正，并严格规范评价流程；
b) 非轻偏差：应参照 7.4.3 采取相应的修正措施。

8 质量管理

8.1 质量控制

DSE体系应包括质量控制活动：

a) 设定 DSE 的质量目标，保证 DSE 的规范、有效；
b) 通过评价机构管控、过程和结果跟踪等手段，监督 DSE 全过程，及时消除质量隐患；
c) 保证 DSE 符合数据（个人信息）安全相关法规、DB21/T 1628、DB21/T XXXX、DB21/T 2702 系列标准的质量保证措施；
d) 为保证 DSE 相关过程、活动的可信、有效、规范所提供的提高评价效能的质量改进措施等。

注2：质量目标应根据不同的书（个人信息）管理者的实际需求设定。

8.2 过程改进

8.2.1 要求

应依据DB21/T XXXX.1第14章的规定并参照DB21/T XXXX.8，采用PDCA过程模式持续改进、完善DSE体系。

8.2.2 方法

DSE体系的过程改进方法应包括：

a) 根据数据（个人信息）管理者的实际，分析、评估DSE目标的可信性，及时修正目标偏差；
b) 根据DB21/T XXXX.4分析评估DSE指标体系的合理性、有效性；
c) 根据DB21/T 1628、 DB21/T XXXX、DB21/T XXXX（评价）分析、评估DSE过程、方法、结果及相关文档资料的规范性、有效性；
d) 根据本文件分析、评估偏差处理的合理性、有效性；
e) 跟踪、追溯DSE全过程，及时发现DSE体系建立、组织、实施、和事后追溯过程的缺陷；
f) 采用PDCA过程模式，修正DSE体系缺陷，持续改进、完善DSE体系等。

8.2.3 评估

评价机构应建立一套评估机制：

a) 质量控制活动的有效性评估；
b) 偏差修正有效性评估；
c) 跟踪、监督DSE过程评估；
d) 过程改进方法评估；
e) DSE体系运行规范性、有效性、可信性和权威性评估；
f) 交流、沟通、意见等的评估等。