ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX.7—XXXX

信息安全技术 数据安全评价 第7部分：现场管理

Information Security technology-data security evaluation part7：site management

（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7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、大连交通大学、大连理工现代工程检测有限公司、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、才昊、李凯、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7部分：现场管理

1 范围

本文件规定了数据安全评价现场审核的评价机构、审核组、审核计划、审核流程、审核实施、风险管理和评估等的规则。

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

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.5 信息安全技术 数据安全评价 第5部分：评价方法

DB21/T XXXX.8 信息安全技术 数据安全评价 第8部分：保证方法

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，重点描述和指导DSE的现场审核管理。

DSE现场审核管理，应以DB21/T 1628系列、DB21/T XXXX标准为基准。

DSE现场审核管理，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现场审核管理，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 评价机构

评价机构应为数据（个人信息）管理者提供现场审核质量保证，主要应包括：

a) 数据（个人信息）管理者基本情况、数据（个人）信息管理情况等的确认；

b) 资格审核文档和结论的真实性、有效性确认；
c) 依据 DB21/T XXXX.3 组建现场审核组、明确审核组职责、考量审核员能力；
d) 现场审核组审核计划的批准；
e) 现场审核过程的控制；
f) 现场审核结论的审查和确认；
g) 现场审核相关的协调和沟通；
h) 接受、处理数据（个人信息）管理者的诉求；
i) 其它必要的质量保证措施等。

6 审核组

6.1 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。审核组应由负责文档审查的审核员担任组长：

a) 审核组长应明确职责和审核组职能；
b) 审核组长应明确 DSE 的目标，并分解目标，分工各位审核员负责；
c) 审核组长应在文档审查中基本了解 DSE 申请者和评价对象的基本情况,并制定现场审核计划；
d) 审核组长应明确质量管控目标和策略，保证 DSE 的质量。

6.2 职责

6.2.1 审核组长

现场审核组组长应明确职责和审核组职能；，组织现场审核：

a) 负责现场审核组 DSE 各阶段的工作；
b) 负责 DSE 管理和质量管控；
c) 依据数据（个人信息）安全相关法规、标准和数据（个人信息）管理者的实际，合理制定审核要求；
d) 根据现场审核要求、评价目标和评价人员的专长、特点等,划分评价人员工作范围,明确职责；
e) 主持编制 DSE 现场审核计划，并组织实施；
f) 根据数据（个人信息）安全相关法规、标准设计评价指标、等级标准、评分范围和权重；
g) 代表现场审核组与数据（个人信息）管理者沟通；
h) 对现场审核各项工作和审核结果做出决定；
i) 提交现场审核报告；
j) 履行评价人员的职责等。

6.2.2 审核员

现场审核组审核人员应包括：应明确职责，履行现场审核分工工作：

a) 工作严谨、实事求是，独立、公平、公正地履行职责；
b) 高质、高效、规范、科学地完成分工范围内的现场审核工作；
c) 了解数据（个人信息）管理者的基本情况；
d) 了解 DSMS（PISMS）构建、实施、运行状况，理解数据（个人信息）管理者实际；
e) 基于 DSMS（PISMS）整体状况，判断、评估分工范围内的 DSMS（PISMS）构成要素；
f) 与分工范围内的数据（个人信息）管理者的相关人员交流、沟通；

g） 与其它审核员交流、沟通；
h） 完成审核组长交付的其它工作等。

6.3 职能

现场审核组的职能，主要应包括：
a） 宣贯 DB21/T 1628、DB21/T XXXX、DB21/T XXXX 系列标准，并释疑解惑；
b） 阐释现场审核计划和审核要求；
c） 遵循 DB21/T XXXX.1、DB21/TXXXX.2、DB21/T XXXX.5，现场审核数据（个人信息）管理与数据（个人信息）安全标准的符合性、有效性；
d） 沟通、协调与现场或相关各方的关系；
e） 形成一致的、符合客观事实的审核结论；
f） 基于 DB21/T XXXX.5、DB21/TXXXX.8 验证审核方式的合理性和有效性；
g） 管理现场审核文档；
h） 安全和保密承诺；
i） 依据 DB21/T 1628.1 谨慎处理敏感的个人信息；
j） 依据 DB21/T XXXX 谨慎处理商业机密信息等。

7 现场审核流程

7.1 要素

基于DB21/T XXXX.1 第9章，现场审核流程要素应包括：
a） 审核员：能力、经验、素质、视角等；
b） 方法：合理性、适用性和有效性；
c） 过程：管控、质量；
d） 事件：分析、评估、处理等。

7.2 流程图

现场审核工作流程，如图1示。

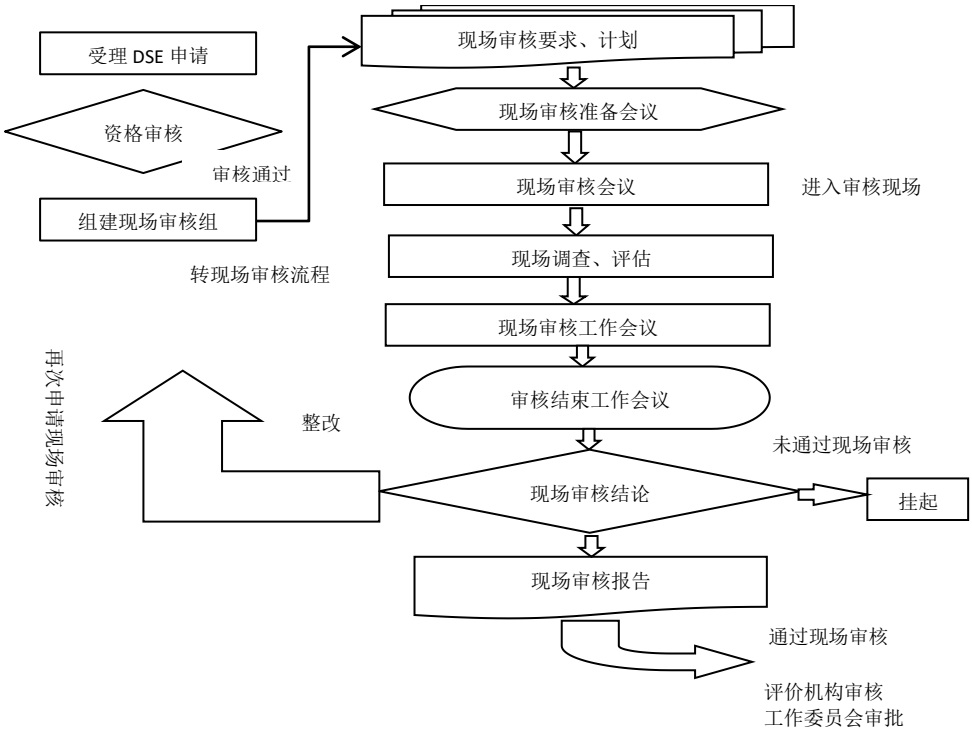

图1　现场审核工作流程

7.3　说明

现场审核工作，主要应完成：

a)　资格审核通过后，评价机构组建现场审核组；
b)　依据数据（个人信息）安全相关法规、标准和 DSE 相关标准，提出并遵守相应的 DSE 要求；
c)　编制 DSE 现场审核计划；
d)　设计评价指标、等级标准、评分范围和权重；
e)　召开现场审核准备会议，明确 DSE 目标、职能职责、工作任务、审核计划、评价指标等；
f)　进入审核现场，召开现场审核工作会议，说明现场审核计划、DSE 要求等各项审核事项；
g)　根据申报文档和资格审核报告，判断、评估并确认申报文档的真实性、一致性；
h)　审核员按照分工要求，调查、分析、判断、评估 DSMS（PISMS）运行状况；
i)　判断数据（个人信息）管理者的数据（个人信息）管理情况与数据（个人信息）安全相关法规、标准及评价要求的符合性；
j)　与数据（个人信息）管理者相关人员沟通、交流；
k)　发现存在的缺陷、隐患，提出整改意见和建议；
l)　召开工作例会，综合评价人员调查、评估意见，研究、讨论不能确认的问题，形成统一的现场审核意见；
m)　验证所采取的现场审核方法的有效性；
n)　审核结束，形成统一的审核结论；
o)　召开工作会议，宣布现场审核结论；
p)　收存和保护与现场审核相关的文档，并按要求提交；
q)　谨慎处理敏感信息（数据）；
r)　编制并提交现场审核报告。

8 审核实施

8.1 要求

DSE现场审核，应依据DB21/T XXXX.1第9章、DB21/T XXXX.5、DB21/T XXXX.8及DB21/T XXXX系列其它标准的规定实施。

8.2 审核计划

现场审核组组长应根据DB21/T XXXX.1 第9章确立的规则，组织编制现场审核计划，并在进入现场后为DSE申请者说明：

a) 审核计划应在完成资格审核，并充分了解 DSE 申请者的相关信息后编制；
b) 审核计划应基于审核员能力、审核过程管理、审核质量控制等的策划；
c) 审核计划应基于资格审核报告确定现场审核的重点、审核方式，制定调查大纲；
d) 审核计划应明确审核双方的要求；
e) 审核计划应充分考虑 DSE 申请者的内、外部条件及对 DSE 的影响；
f) 审核计划应明确审核质量管理、安全管理、文档管理等的有效方法等。

8.3 人员要求

DB21/T XXXX.1 第9章确定了审核双方人员的基本要求：

a) 现场审核人员要求，应包括个人修养、业务素质、专业水平、评价能力等；
b) 调查样本人员要求，应包括基本素质、诚信品质、业务能力等。

8.4 审核流程

8.4.1 流程准备

进入审核流程前，应完成相应的准备工作：

a) 编制 DSE 现场审核计划；
b) 设计、建立评价指标体系和相应的权重；
c) 确定现场审核等级标准和评分范围；
d) 设计调查方法和调查大纲；
e) 资格审核存在问题的处理；
f) 相关文档管理等。

8.4.2 流程展开

应依据DB21/T XXXX.1 第9章展开流程管理，主要应包括：

a) 现场审核项的归类和分工；
b) 审核会议的相关准备；
c) 审核过程的控制、协调、沟通；
d) 审核偏差处理；
e) 审核员的工作协同；
f) 审核意见的一致性协调；
g) 审核结论的说明；
h) 其它必要的管理等。

8.4.3 流程改进

审核组应考虑审核流程的修正、改进、完善：

a) 现场审核过程中可能存在的缺陷、风险、事件等应及时修正、改进；

b) 或审核结束后、或定期回溯审核过程，发现问题应随时改进、完善，并提供经验积累。

8.5 审核质量

8.5.1 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（个人信息）管理者的数据（个人信息）安全状况。

8.5.2 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（个人信息）安全相关法规、标准和数据（个人信息）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（个人信息）管理现状、缺陷、漏洞、隐患和影响等。

8.5.3 问题处理

在现场审核过程中，应及时处理影响DSE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等。

8.5.4 调查偏差

依据DB21/T XXXX.1第9章，偏差类型可包括：

a) 整体偏差：

   1) 总体设计偏差：现场审核计划、现场调查方案等的设计中，相关信息不完备或主管意识偏差可能引发的审核偏差；

   2) 系统偏差：在现场审核过程中的各个环节，存在多种因素影响审核调查质量，如审核人员素质、知识、技术、经验、调查技巧、心理因素等；

b) 随机偏差：

   1) 技术偏差：如法规标准的可操作性、调查方法选择、文字表述等可能产生的偏差；

   2) 样本选择偏差：样本选择策略偏差、样本范围偏离目标和原则、样本数量不适当、样本抽查方法不适当等引发的时候偏差等。

8.5.5 调查控制

现场审核偏差控制，主要应：

a) 依据 DB21/T XXXX.1 9.4 采取相应的控制措施；
b) 依据 DB21/T 2702.1 9.4 及时处理各种可能的问题；
c) 注意审核员个人素养养成，包括知识、技术、经验、调查技巧、表达能力、沟通交流能力、行为偏差控制等；
d) 依据 DB21/T XXXX.1 9.4，与 DSMS（PISMS）相关人员沟通交流，与审核组内成员互动交流等。

8.5.6 沟通交流

在现场审核过程中，应与数据（个人信息）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、评估观点等。

8.6 审核意见

8.6.1 要求

应依据DB21/TXXXX.2 10.4.5.3形成公正审核结论。

8.6.2 意见

应依据DB21/T XXXX.1 9.5，基于审核结论形成现场审核意见：

a) 应依据 DB21/T XXXX.2 8.3、8.4 确定评分等级、评分范围；
b) 应依据 DB21/T XXXX.2 第 8 章、DB21/T XXXX.4 第 7 章，计算各个评价指标累加总分，并加权计算，获得评价总分；
c) 应依据 DB21/T XXXX.1 9.5 确立的规则和评价总分，评估评价对象的评价等级；
d) 如满足 DB21/T XXXX.1 9.5.3 a）1）的条件，应通过 DSE；
e) 形成现场审核意见等。

8.6.3 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，并依据DB21/T XXXX.1 9.6.2提交整改报告。

现场审核组应评估整改报告：

a) 如已满足 DB21/TXXXX.1 9.5.3 a）1）的条件，应通过 DSE；
b) 应根据 DB21/T XXXX.1 9.5.3 a）3）确立的原则，再次现场审核；
c) 根据 DB21/T XXXX.1 9.5.3 b）1）确立的原则，如仍不能达到 DB21/T XXXX.1 9.5.3 a）1）的条件，不应通过现场审核等。

8.7 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。

9 风险管理

9.1 风险识别

9.1.1 审核准备

进入现场审核的准备阶段，可能存在的风险主要包括

a) 资格审核：资格、文档审查漏项、审核结论的偏差等；
b) 审核计划：计划的完整性、适用性等；
c) 评价指标：评价指标的合理性、适用性、有效性，权重设计的符合性等；
d) 管理机制：现场审核组的职责、职能、现场管理措施的设计缺陷等；
e) 其它可能的风险等。

9.1.2 审核过程

现场审核过程可能存在的风险主要包括：

a) 审核员：能力、素质、视角等；
b) 调查方法：调查大纲的合理性、调查方法运用的偏差、调查样本选择的代表性、沟通技巧等；
c) 审核流程：审核流程设计缺陷、流程展开偏差等；
d) 工作机制：审核员协同缝隙、审核偏差等；
e) 审核质量：审核质量管控措施的缺陷、有效性等；
f) 过程管理：审核组职能职责履行缺陷、审核过程管理失误等；
g) 其它可能的风险等。

9.1.3 审核结论

现场审核意见、结论可能存在的风险，主要包括：

a) 审核结论：审核员素质偏差、视角偏差等；
b) 审核等级：等级设计、评分范围的合理性等；
c) 审核意见：审核意见的有效性等；
d) 其它可能的风险等。

9.2 风险控制

9.2.1 评价机构

评价机构应评估、控制现场审核风险：

a) 应根据 DSE 申请者的实际需要，选聘能力、业务、经验等适合的现场审核组组长和审核员；
b) 应依据 DB21/T XXXX 系列标准，规范通用的现场审核组职能、职责及现场审核管理机制，并审查、批准特定需求的剪裁、修改；
c) 应检查、确认资格审核无误，批准资格审核报告；
d) 应审核、批准现场审核计划；
e) 应监控现场审核过程，随时处理应急事件；
f) 应审查、评估、确认现场审核意见的符合性、有效性；
g) 其它应监控的风险等。

9.2.2 审核准备

在现场审核准备阶段应监控并及时处理风险：

a) 审核组应充分了解、熟悉 DSE 申请者的基本情况；
b) 审核组应充分了解、掌握 DSE 申请者数据（个人信息）管理状况和可能存在的缺陷；
c) 审核组应充分理解、评价 DSE 申请者的数据（个人信息）管理计划、DSMS（PISMS）内审报告、体系运行报告；

d) 应评估、判断资格审核缺陷部分的整改结果；
e) 应依据 DB21/T XXXX.4 评估评价指标体系设计的符合性、合理性；
f) 应建立现场审核组内部沟通机制，避免审核意见相悖；
g) 审核组长应具有风险掌控能力，及时发现、修正现场审核准备阶段的风险等。

9.2.3 审核过程

在现场审核过程中监控并及时处理风险，主要包括：
a) 应实际了解审核现场的实际状况；
b) 应与最高管理者、管理代表、数据（个人信息）管理责任主体等充分沟通、交流；
c) 应明确审核员现场审核分工和审核组内的沟通机制；
d) 应确定现场审核相关资源配置的充分性；
e) 应确定重点审核项的符合性、合理性；
f) 应依据 DB21/TXXXX.8 控制现场审核质量；
g) 应在现场管理中适时调整、修正过程要素；
h) 审核组长应随时评估现场审核可能存在的风险，及时改进等。

9.2.4 审核结束

现场审核结束时，应检查、评估现场审核可能存在的风险：
a) 应梳理、检查、评估审核过程的规范性、有效性；
b) 应确认现场审核风险在可控范围内；
c) 应依据 DB21/T XXXX.8 控制、调整可能存在的审核偏差；
d) 应确认审核意见的合理性、客观性和有效性；
e) 应与 DSE 申请者相关人员充分沟通；
f) 其它必要的风险控制措施。

10 评估

DSE结束后，应定期或不定期回溯DSE过程，检查、分析、评估可能存在的缺陷、风险，持续改进、完善DSE过程。