ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX.3—XXXX

信息安全技术 数据安全评价 第3部分：审核员管理

Information Security-Personal information security management system evaluation part3：auditor management

（征求意见稿）

（本草案完成时间：2023-01-10）

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3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3部分：审核员管理

1 范围

本文件规定了数据安全评价的评价人员及相应的职业规范、资格管理、注册管理、培训管理、资格审核等规则。

本文件适用于各类数据（个人信息）安全评价机构。

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，亦遵循DB21/T XXXX.2规范的DSE实施指南，重点描述和指导DSE人员管理的约束规范。

DSE人员，应遵循DB21/T 1628系列标准、DB21/T XXXX.1及相应的标准系列的基本规则。

DSE人员管理，应基于DB21/T XXXX.1、和本文件的基本规则，并参照DB21/T XXXX（评价）系列其它标准。

DSE人员管理，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的认证人员管理规则。

5 评价人员

5.1 称谓

DSE人员宜称为DSE审核员。

5.2 类别

5.2.1 分类

审核员应分为2类：

a) 审核管理人员：包括DSE评价机构、DSE培训组织、DSE咨询组织的管理人员等；
b) 审核专业人员：包括DSE审核员、DSE咨询人员、DSE培训人员等。

5.2.2 分级

DSE审核员应遵循DB21/T XXXX.1 12.3，根据业务能力、专业能力和从业经验等分级，宜分为3级：

a) 主任审核员：管理、领导专业审核工作的评价人员；
b) 审核员：专业审核的评价人员；
c) 实习审核员：准备成为审核员的评价人员等。

6 职业规范

审核员应遵守职业规范：

a) 应在国家法规框架内，独立、客观、公正、科学、规范地行使评价人员的职能；
b) 应修正、提高职业操守和执业能力，适应不同工作环境的能力需求；
c) 无法律要求或DSE申请方的书面授权，应保守评价相关的任何信息；
d) 不应传播可能损害评价双方利益的虚假或误导性信息；
e) 不应接受DSE申请方任何相关人员或任何利益相关方的任何馈赠或其它利益输送；
f) 其它必须遵守的职业规范。

7 管理

7.1 要求

评价机构应遵循DB21/T XXXX.1第12章，建立审核员管理机制，以保证DSE的质量、专业、效果。

7.2 职能

评价机构的审核员管理职能，主要应包括：

a) 评价机构统一管理审核员的聘任、考核、监督，及行为、能力、业绩等的评估；
b) 评价机构统一规范审核员能力、知识等技能提高的培训、教育等；
c) 评价机构统一管理审核员相关的争议事项；
d) 评价机构统一颁发、管理评价人员执业资格证书等。

7.3 制度

评价机构应遵循DB21/T XXXX.1第12章，建立审核员管理制度，主要应包括：

a) 审核员的注册、资格、等级认定；
b) 审核员的职责、义务；
c) 审核员的行为规范；
d) 审核员的聘任规则；
e) 审核员的行为、能力、业绩评估；
f) 审核员的知识能力、专业技能；
g) 审核员的考核规则；

h) 审核员培训教育；
i) 审核员争议事项处理；
j) 审核员资格管理；
k) 评价管理人员的管理等。

7.4 人员

评价管理人员应从审核员中选择、聘用。

8 资格取得

8.1 基本资格

审核员应具备的基本资格，主要应包括：
a) 具备完全民事行为能力；
b) 遵守国家法律，严谨、科学、公正，实事求是，具有良好的职业素养；
c) 具有一定的职业、专业教育经历，具备信息安全相关专业知识、个人信息安全基本知识等专业素质和完成认证必须的基本技能；
d) 通过评价机构的培训，并取得执业资格证书；
e) 评价机构确定的其它规定等。

8.2 基本能力

8.2.1 实习审核员

实习审核员应具备的基本能力，主要应包括：
a) 应具有 2 年以上的相关工作经验；
b) 应理解个人信息安全相关法规、标准的基本概念、基本内涵，及 DSE 中的应用；
c) 应独立完成 DSMS（PISMS）和 DSE 相关咨询工作；
d) 应辅助完成 DSE 审核组的相关工作等。

8.2.2 审核员

审核员应具备的基本能力，主要应包括：
a) 应具备 8.2.1 的基本能力，并有 2 年实习审核员经验；
b) 应熟练掌握、解读个人信息安全相关法规、标准，及 DSE 中的应用；
c) 应独立指导 DSMS（PISMS）的建设、实施；
d) 应熟悉 DSE 全过程，并应独立完成所负责的 DSE 工作；
e) 应熟悉并完成 DSE 的相关文档的编制和管理等。

8.2.3 主任审核员

主任审核员应具备的基本能力，主要应包括：
a) 应具备 8.2.2 的基本能力，并有 5 年审核员经验；
b) 应组织、领导、管理 DSE 全过程，并提出建设性意见；
c) 应组织、指导审查、编制 DSE 完全文档；
d) 主持审核工作后，应向评价机构报告 DSE 活动和结果，并提交相关文档；
e) 可主持、参与个人信息安全相关法规、标准的相关工作等。

9 注册

9.1 要求

评价机构应建立审核员注册制度：

a) 申请 DSE 审核员资格证书，应经过评价机构注册；
b) 评价机构应依据本文件审核申请人资格的有效性；
c) 评价机构应对申请人相关资料实行备案管理；
d) 评价机构应以适当方式公布取得审核员资格证书的申请人，以供选聘；
e) 应在申请人资格审核通过后颁发相应等级的审核员资格证书。

9.2 实习审核员

实习审核员申请注册，应：

a) 已具备本文件规定的资格；
b) 应参与 DSE 实习 3 次以上；
c) 应接受个人信息安全相关专业培训 2 次以上，并取得合格证书；
d) 应提交注册规定的相关文档，主要包括：
    1) 实习审核员申请表；
    2) 培训合格证书；
    3) 实习报告；
    4) 主任审核员书面签署意见等。

9.3 审核员

审核员申请注册，应：

a) 已具备本文件规定的资格；
b) 应全程参与 DSE5 次以上，并应独立完成相关的辅助工作，如文档编制、协助审查等；
c) 应接受 DSE 审核员培训，并取得合格证书；
d) 应有 2 名主任审核员推荐；
e) 应提交注册规定的相关文档，主要包括：
    1) 审核员申请表；
    2) 培训合格证书；
    3) 实习审核员资格证书；
    4) 主任审核员推荐书；
    5) 评价工作报告等。

9.4 主任审核员

主任审核员申请注册，应：

a) 已具备本文件规定的资格；
b) 应全程参与 DSE10 次以上；
c) 应实习主任审核员的职责，并应胜任相应工作；
d) 应接受 DSE 主任审核员培训，并取得合格证书；
e) 可参加 DSE 研讨，并提出独立见解；
f) 宜有 DSE 相关标准编制参与经验；

g) 应有 2 名主任审核员推荐；
h) 应提交注册规定的相关文档，主要包括：
   1) 主任审核员申请表；
   2) 培训合格证书；
   3) 审核员资格证书；
   4) 主任审核员推荐书；
   5) 审核员工作报告；
   6) DSE 相关业绩说明；
   7) 工作案例说明等。

9.5 时限

评价机构应规定注册相关的时限：
a) DSE 实习审核员取得培训合格证书后，申请注册的有效时限应为 3 个月；
b) 取得 DSE 审核员培训合格证书的时间不应早于审核员申请注册前 3 个月；
c) 取得 DSE 主任审核员培训合格证书的时间不应早于主任审核员申请注册前 3 个月。
d) 实习审核员的工作年限宜为 3 年；
e) 审核员的工作年限宜为 5 年等。

10 资格审核

10.1 要求

管理机构应委托评价机构对获得审核员资格证书人员的技术和业务能力实施年度审核，以确定审核员的工作能力和工作适应性。

10.2 内容

年度资格审核的内容，主要应包括：
a) 依据本文件审核审核员的业务能力、知识能力；
b) 依据本文件审核审核员接受培训、知识更新；
c) 依据本文件审核审核员的实践能力；
d) 依据本文件审核审核员的基本素质、工作事故等。

10.3 事故处理

10.3.1 事故

年度内审核员出现重大工作失误、事故， 主要可包括：
a) DSE、咨询过程中，没有履行相应的工作职责，受到投诉；
b) DSE 过程中出现重大失误；
c) 私相授受 DSE 相关信息；
d) 私下接受利益相关方馈赠等。

10.3.2 处理

DSE事故的处理，主要应包括：
a) 一般性、未造成影响的失误，应给予警示或警告；

b） 一般性、无重大过错的投诉，应给予警告；
c） 出现重大失误、存在严重过错的投诉，应视情节给予降级、取消审核员资格处分；
d） 未通过年度资格审核，应重新参加培训，并重新申请相应等级的审核员资格等。

注1：取消审核员资格后，三年内不应重新申请，再次申请时，应自实习审核员始。

11 培训

11.1 要求

评价管理机构应委托评价机构定期或不定期实施不同等级审核员的培训，以提高审核员的专业技能和业务能力：

a） 应根据不同审核员等级，确定不同的培训要求；
b） 应根据不同的培训要求制定相应的培训计划；
c） 应根据培训实际改进、完善培训计划，保证培训的有效性和适应性。

11.2 内容

11.2.1 实习审核员

实习审核员培训应是审核员执业的基础培训，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）安全基本知识；
c） DSMS（PISMS）、DSE 基本知识；
d） DSE 工作流程；
e） 其它业务知识等。

11.2.2 审核员

审核员培训主要应包括：

a） 数据（个人信息）安全相关法规与相关标准的关系；
b） 数据（个人信息）管理知识；
c） DSE 过程管理；
d） 数据（个人信息）安全风险管理；
e） 其它专业和业务知识等。

11.2.3 主任审核员

主任审核员培训主要应包括：

a） DSE 的组织、管理；
b） 数据（个人信息）安全变化趋势的应对；
c） DSMS（PISMS）与其它管理体系的融合；
d） 数据（个人信息）安全标准的编制等。

11.3 方式

审核员的培训方式，应包括：

a） 授课：评价机构应依据 11.2 设计课程，组织授课；
b） 实践：包括：

1） 模拟：授课现场模拟实践教学；

2） 现场：随审核组现场辅助审核等；

c） 讲评：针对 DSE 过程中的问题展开讲解、讨论；

d） 研讨：针对典型案例、或有争议的问题、或设定课题，展开讨论等。

注2：应根据不同等级的审核员采取不同的培训方式。

12 证书管理

审核员资格证书的有效期应为3年，审核员在DSE中无重大失误、事故，且通过年度考核，应在3年后申请更换。