ICS 35.020
L70

DB21

辽　宁　省　地　方　标　准

DB 21/T 2702.6—XXXX

信息安全 个人信息安全管理体系评价 第6部分：资格审核

Information security-Personal information security management system evaluation part6：Qualification audit

（征求意见稿）

（本稿完成日期：2017-4-4）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省质量技术监督局　发布

目　　次

前　言

DB21/T 2702 分为 11 部分：

—信息安全 个人信息安全管理体系评价 第 1 部分：要求

—信息安全 个人信息安全管理体系评价 第 2 部分：管理指南

—信息安全 个人信息安全管理体系评价 第 3 部分：评价员管理

—信息安全 个人信息安全管理体系评价 第 4 部分：评价指标

—信息安全 个人信息安全管理体系评价 第 5 部分：评价方法

—信息安全 个人信息安全管理体系评价 第 6 部分：资格审核

—信息安全 个人信息安全管理体系评价 第 7 部分：现场管理

—信息安全 个人信息安全管理体系评价 第 8 部分：保证方法

—信息安全 个人信息安全管理体系评价 第 9 部分：仲裁指南

—信息安全 个人信息安全管理体系评价 第 10 部分：审批指南

—信息安全 个人信息安全管理体系评价 第 11 部分：资格管理

本部分是 DB21/T 2702 的第 6 部分。

本部分按照 GB/T1.1—2009《标准化工作导则　第 1 部分：标准的结构与编写》给出的规则起草。

本部分由大连市经济和信息化委员会提出。

本部分由辽宁省经济和信息化委员会归口。

本部分主要起草单位：大连软件行业协会、大连交通大学

本部分主要起草人：郎庆斌、孙鹏、尹宏、丁宗安、董晶、杨万清、杨莉、郭玉梅、曹剑、司丹、孙毅、王小庚。

信息安全 个人信息安全管理体系评价 第6部分：资格审核

1 范围

本标准为实施个人信息安全管理体系评价申请资格审核提供指导和通用规则。

本标准适用于各类个人信息安全管理体系评价机构，亦为已建立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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 1628.1 信息安全 个人信息保护规范

DB21/T 1628.2 信息安全 个人信息安全管理体系 第2部分：实施指南

DB21/T 2702.1 信息安全 个人信息安全管理体系评价 第1部分：要求

DB21/T 2702.2 信息安全 个人信息安全管理体系评价 第2部分：管理指南

3 术语和定义

DB21/T 1628、DB21/T 2702界定的以及下列术语和定义适用于本文件。

3.1

资格 qualification

为申请PISMSE应具备的条件和PISMS活动过程。

3.2

资格审核 evaluation

分析、判断、评估申请PISMSE应具备的条件和PISMS活动。

4 要求

本指南遵循 DB21/T 2702.1 确立的 PISMSE 的基本原则和要求，重点描述和指导申请 PISMSE 资格审核的约束规范，具体要求应符合：

a）PISMSE 资格审核，应以 DB21/T 1628 系列标准为基准；

b）PISMSE 资格审核，应同时使用 DB21/T 2702.1 和本指南，并参照 DB21/T 2702 系列其它标准；

c）PISMSE资格审核，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 申请资格

5.1 主体特征

个人信息管理者是申请PISMSE的主体，其主体特征应如DB21/T 1628.2 9.1节所述：

a）合法、有效、独立的机关、企业、事业、社会团体等组织；

b）个人；

c）具有民事权利和民事能力，享有民事义务，承担民事责任；

d）具有公共管理职能。

5.2 相关资格

个人信息管理者申请PISMSE所需的相关资格，主要应包括：

a）法律、法规、标准（规范）的遵从性；

b）组织管理的规范性、科学性；

c）体系管理的充分性、规范性、有效性；

d）员工的个人信息安全认知性；

e）最高管理者、管理者的个人信息安全认知性等。

6 申请条件

6.1 社会角色

在社会形态中，个人信息管理者的角色，主要应包括：

a）主体特征合法、合规；

b）个人信息管理者运行正常，风险可控；

c）个人信息管理者遵循DB21/T 1628.2 9.1.2节规定，承担相应的责任和义务。

6.2 相关条件

个人信息管理者申请PISMSE应具备的相关申请条件，主要应包括：

a）相关资格确认；

b）申请PISMSE的个人信息管理者依据个人信息安全相关法规、标准和实际需要构建、实施了PISMS；

c）申请PISMSE前未发生个人信息安全相关事故、事件；

d）申请PISMSE前，PISMS应正常、安全、有效运行3个月以上；

e）申请PISMSE前，PISMS应经过内审和评估，无重大、实质性安全隐患；

f）申请PISMSE前存在的个人信息安全隐患、缺陷应有效整改、完善；

g）申请PISMSE的个人信息管理者根据实际需求主动申请PISMSE等。

7 受理机构

7.1 要求

PISMSE申请，应由评价机构受理。评价机构依据DB21/T 2702.1 8.1.2审核申请PISMSE的个人信息管理者的资格，确认申请PISMSE的个人信息管理者具有PISMSE申请资格：

a）依据DB21/T 2702.2，评价机构应是管理主体指导、批准设立的管理机构，为管理、实施PISMSE派出的评价主体；

b）评价机构应依据DB21/T 2702.2 6.3.4建立了相对完善的管理机制；
c）依据DB21/T 2702.2 6.4，评价机构应具有一定的组织能力，并配备相应的评价员队伍；
d）评价机构应依据DB21/T 2702.2 第7章，建立了完善的评价体系，并制定了相应的评价规则；
e）评价机构宜依据DB21/T 2702.2 第9章，建立PISMSE指标体系。

7.2 责任和义务

7.2.1 责任

依据DB21/T 2702.2，评价机构应承担的责任和义务主要包括：
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。
b）法律责任：
评价主体应承担和履行评价过程中保证个人信息安全的法律责任，避免因评价引发个人信息主体权益受损。

7.2.2 义务

评价主体应承担的相应义务主要包括：
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，保证评价质量和个人信息主体权益所应遵循的相关法规、标准。

7.3 审核管理

7.3.1 职责

评价机构应遵循DB21/T 2702.2 6.3.4.4确立的职责。

7.3.2 管理制度

评价机构应遵循DB21/T 2702.2 6.3.4.5的规则，建立相应的管理制度。

7.3.3 审核活动

7.3.3.1 活动组织

评价机构应遵循DB21/T 2702.2 6.4.的规则，组织PISMSE资格审核相关活动，主要应包括：
a）明确职责和行为规范：受理活动的行为准则；
b）受理活动：依据相关标准受理PISMSE申请；
c）资格审核：PISMSE申请者申请资格审核；
d）受理评估：评估受理质量、效果、效率；
e）后处理：
1）选择适宜的评价人员；
2）组建现场审核组；

3）评价后的其它相关工作；

f）其它：其它需要完成的工作等。

7.3.3.2 控制和协调

评价机构应遵循DB21/T 2702.2 6.5、6.6节的规则，控制资格审核过程，协调相关事宜。

8 审核构成

PISMSE资格审核，由2部分构成：

a）资格审查：确认申请PISMSE的个人信息管理者是否具备PISMSE申请资格；

b）文档审查：申请PISMSE的个人信息管理者提交审查的个人信息管理相关文档的完整性、规范性、有效性审查。

9 接受申请

评价机构应依据DB21/T 1628、DB21/T 2702系列标准（包括本标准）接受PISMSE申请，并应于15日内决定是否受理申请：

a）受理申请应书面通知PISMSE申请者，说明已受理PISMSE申请，将开展PISMSE相关活动；

b）不受理申请，应书面通知PISMSE申请者，说明原因。

10 资格审核

10.1 资格审查

10.1.1 要求

评价机构接受PISMSE申请后，应组织评价机构相关人员，审查、评估申请PISMSE的个人信息管理者的申请资格、申请条件等，以判断申请PISMSE的个人信息管理者是否具备PISMSE申请资格。并确定是否受理申请。

10.1.2 审查方式

10.1.2.1 概述

资格审查可以采用多种方式，综合评估申请PISMSE的个人信息管理者的评价资格，以获得相对公允的审查结果。

10.1.2.2 面谈

评价机构人员可在申请PISMSE的个人信息管理者提交申请时面谈，了解申请PISMSE的个人信息管理者的基本情况、个人信息管理的一般情况，以及个人基本素质等。

面谈可以形成对申请PISMSE的个人信息管理者的基本认知，但不应形成偏见。

10.1.2.3 检查文档

依据DB21/T 1628、DB21/T 2702系列标准，检查申请PISMSE的个人信息管理者提交文档的完整性、规范性、可信性。

10.1.2.4 其它

可采取其它方式，辅助资格审查，如利用网络、登录个人信息管理者网站等，了解申请PISMSE的个人信息管理者的基本情况。

10.1.3 申请资格

10.1.3.1 要求

申请PISMSE的个人信息管理者申请PISMSE，应满足第6章的规定，并提供相关说明。评价机构可在资格审核中初步确认。

10.1.3.2 特征审查

10.1.3.2.1 应提交的文档

个人信息管理者应提交的文档，主要包括：

a）PISMSE申请表；

b）申请PISMSE的个人信息管理者的相关资质等；

c）申请PISMSE的个人信息管理者的基本情况说明等。

10.1.3.2.2 审查

应采用10.1.2.2、10.1.2.4的方法，审查、评估申请PISMSE的个人信息管理者的基本情况、申报基本情况的真实性、可信性。

10.1.3.3 相关资格审查

相关资格审查，可采取几种方式了解、判断、综合评估，初步确认相关资格各项：

a）采用10.1.2的方法，综合判断；

b）利用10.1.3.2.2的审查结论等。

10.1.4 文档检查

10.1.4.1 申报文档

申请PISMSE的个人信息管理者，应依据DB21/T 1628、DB21/T 2702系列标准准备并提交PISMSE相关的文档，主要应包括：

a）依据DB21/T 1628.1第7章，提交个人信息管理相关文档，主要应包括：

1）个人信息管理计划；

2）个人信息管理相关的文档、包括记录、人事关系等；

b）个人信息管理文档与标准对应表；

c）依据DB21/T 1628.1第8章、第9章、第10章、第11章，提交PISMS相关文档：

1）管理机制相关文档，如制度、培训教育等；

2）个人信息数据库相关文档和说明；

3）与管理、业务相关个人信息相关文档，如个人信息获取、处理、提供等；

4）个人信息安全管理的相关文档；

5）过程管理相关文档，如内审、过程改进等；

6）PISMS的其它相关文档，包括记录、表格、统计报表等；

d）依据DB21/T 2702.1 7.1.2，提交PISMS内审报告和体系运行报告；

e）PISMS整改、个人信息安全事故等相关报告；
f）PISMS风险管理报告；
G．其它需要说明的问题等。

10.1.4.2 审查

应采用10.2的方法，审查、评估申请PISMSE的个人信息管理者提交文档规范性、完整性、真实性和可信性。

10.1.5 资格评估

10.1.5.1 要求

应通过特征检查、文档检查，综合评估申请PISMSE的个人信息管理者的申请资格。

10.1.5.2 结论

通过评估获得的资格审查结论，主要应包括：
a）同意受理申请，确认具备PISMSE资格：
1）提交特征审查的文档真实、有效；
2）主体资格合法、合规；
3）申报文档规范、完整、真实、可信；
b）存在以下问题之一，应改进、完善后重新评估：
1）提交特征审查的文档存在缺陷、漏项、不完整；
2）申报文档不规范等；
c）存在以下问题之一，不予受理，并书面通知申请PISMSE的个人信息管理者，说明原因：
1）申报文档存在重大隐患（如虚报、瞒报等）；
2）申报文档粗制滥造等。

10.1.5.3 报告

资格审查结束后应将形成的资格审查结论，提交文档审查人员参考。

10.2 受理申请

10.2.1 受理通知

依据10.5.2结论a，评价机构同意受理通过资格审查的申请PISMSE的个人信息管理者的申请，并书面通知申请PISMSE的个人信息管理者。

10.2.2 受理工作

受理申请PISMSE的个人信息管理者的PISMSE申请后，评价机构应选聘具有相应能力的评价人员，审查申请PISMSE的个人信息管理者提交的PISMSE申报文档，并开始组织PISMSE相关活动。

10.3 文档审查

10.3.1 概述

文档审查应是评价机构选聘的评价人员，依据DB21/T 2702.1、DB21/T 2702.确立的资格审核规则和内容，独立、客观的理解、评估申请PISMSE的个人信息管理者申报的文档，形成公允的审查结论。

10.3.2 摘要

10.3.2.1 计划审查

基于申请PISMSE的个人信息管理者的基本情况审查，评估：

a）个人信息管理计划的完整性、充分性和有效性；

b）资源能力的有效性和效率；

c）最高管理者的认知等。

10.3.2.2 数据库审查

基于申请PISMSE的个人信息管理者的基本情况审查，评估：

a）个人信息源识别的充分性；

b）个人信息数据库设计、构建的规范性、合理性、可信性；

c）个人信息数据库管理的合理性、规范性、安全性等。

10.3.2.3 标准对应审查

基于个人信息管理文档与标准规则对应表审查，评估：

a）规则对应的适应性、一致性；

b）申请PISMSE的个人信息管理者个人信息安全认知、理解和能力等。

10.3.2.4 机制审查

基于PISMS相关文档审查，评估：

a）管理机制的健全性、合理性；

b）管理制度的完整性、符合性和一致性；

c）员工和与个人信息管理相关人员管理的规范性、科学性；

d）宣传教育的有效性；

e）文档管理的规范性、可用性。

10.3.2.5 业务审查

基于PISMS相关文档审查，评估：

a）与个人信息相关的管理、业务的可控性、可信性；

b）与个人信息相关的管理、业务关联因素的可控性、安全性；（如与社会互联、移动个人信息数据库等）

c）个人信息利用（委托、提供、交易、二次开发等）的可控性、可信性、安全性等。

10.3.2.6 过程管理审查

基于PISMS相关文档审查，评估：

a）基于个人信息生命周期的过程管理的有效性、安全性；

b）PISMS过程改进的可信性、有效性；

c）内审过程的可控性、充分性等。

10.3.2.7 体系审查

基于PISMS运行报告、内审报告等，评估体系管理的充分性、有效性、适宜性。

10.3.2.8 风险审查

基于风险管理报告，评估：

a）风险识别、分析、管理的可信性、充分性和有效性；

b）PISMS的风险可控性、残余风险可控性等。

10.3.3 审查评估

10.3.3.1 评估要求

应基于10.3.2，初步评估文档审查的结果：

a）申请PISMSE的个人信息管理者个人信息管理的有效性和法规、标准的符合性；

b）明确审查、评估过程中确认的需要整改的问题；

c）明确审查、评估过程中无法确认，需要通过现场审核确认的问题；

d）形成文档审查结论等。

10.3.3.2 结论

通过评估获得的文档审查结论，主要应包括：

a）可以通过文档审查：

1）初步评估个人信息安全隐患、缺陷等得到有效整改、完善；

2）无个人信息安全事故；

3）初步评估个人信息管理、PISMS运行符合个人信息安全相关法规、标准；

b）经过整改、完善后重新评估：

1）初步评估个人信息管理、PISMS运行存在缺陷；

2）初步评估个人信息安全隐患、缺陷等未得到有效整改；

c）不能通过文档审查：

1）初步评估个人信息管理、PISMS运行存在重大缺陷；

2）初步评估个人信息安全存在重大隐患、缺陷；

3）存在重大个人信息安全事故的可能性等。

10.4 审核结论

10.4.1 要求

应整合资格审查、文档审查结论，综合评估申请PISMSE的个人信息管理者的申请资格。

10.4.2 审核合格

资格审核满足下列条件的，应予合格：

a）满足第6章的申请条件；

b）PISMS相关文档规范、完整、真实、有效；

c）PISMS实施、运行状况良好；

d）个人信息管理有效，符合个人信息安全相关标准、法规；

e）PISMS运行存在可接受的非实质性问题;

f）资格、文档审查合格。

10.4.3 基本合格

资格审核符合下列条件的，应要求个人信息管理者修改、改进、完善后重新提交审核：

a）不能完全满足第6章的申请条件；

b）PISMS相关文档存在缺陷，需要改进、完善；

c）PISMS实施、运行存在某些需要改进、完善的问题；

d）存在某些需要现场评价确认的一般性问题；

e）资格、文档审查需要改进。

10.4.4 不合格

资格审核中发现存在下列问题，评价机构应退回申报材料，并要求个人信息管理者重新内审、自我评价，达到评价要求后重新申请PISMSE：

a）不能满足第6章的申请条件；

b）PISMS相关文档存在重大隐患（如虚报、瞒报等）；

c）PISMS实施、运行存在重大缺陷：

1）事故等级较高；

2）事故处理措施不当；

3）发生重大个人信息安全事故，且尚在恢复期；

d）资格、文档审查不合格。

注1：本节改写自 DB21/T 2702.1 8.2.

10.5 审核报告

10.5.1 不合格项报告

申请PISMSE的个人信息管理者申请PISMSE基本合格的，应形成不合格项报告：

a）资格审核中存在的问题、缺陷、安全风险等的说明；

b）问题、缺陷、安全风险等的分析；

c）需要现场确认的问题说明；

d）整改建议等。

10.5.2 退回报告

评价机构退回申请PISMSE的个人信息管理者申报的PISMSE材料，应形成不合格退回报告：

a）资格审核中存在的重大隐患、缺陷、安全风险等的说明；

b）重大隐患、缺陷、安全风险等的分析；

c）退回原因说明；

d）退回后应实施的主要工作说明；

e）整改建议等。

10.5.3 资格审核报告

完成资格、文档审查后，应编制资格审核报告，主要内容包括：

a）申请PISMSE的个人信息管理者申请资格审查情况说明；

b）申请PISMSE的个人信息管理者提交文档审查情况说明；

c）初步评估PISMS实施、运行状况；

d）个人信息安全相关法规、标准的符合性；

e）个人信息安全风险管理情况说明；

f）审核结论说明：

1）审核合格；

2）基本合格：

•不符合、不满足PISMSE要求事项说明；

•应现场确认问题说明

•申请PISMSE的个人信息管理者整改情况说明；

•申请PISMSE的个人信息管理者出具的整改报告；

3）不合格

•不合格说明；

•退回说明。

注2：本节改写自 DB21/T 2702.1 8.3。

注3：资格审核报告格式，可参考 DB21/T 2702.1 附录 E。

11 评估

11.1 要求

评价机构应定期评估资格审核过程，及时处理资格审核过程中出现的问题、缺陷，改进和完善资格审核过程、提升资格审核质量。

11.2 质量评估

11.2.1 客观性

在资格审核中，应避免因受外界因素、主观思维的影响，评估、判断出现偏差。在评估资格审核质量时，应检查、判断资格审核过程的独立性，评估审核方法的客观性。

11.2.2 软评价

在资格审核中，知识、专业、经验等可能影响客观判断、评估。在评估资格审核质量时，应基于审核人员的知识、专业、经验等，考虑评价人员的审核视角，评估审核过程的主观认知和客观事实的一致性。

11.3 效果评估

11.3.1 影响因素

可能影响资格审核效果的主、客观因素，继承资格审核过程的独立性、客观性。评价机构应评估影响因素对审核结果的影响，判断资格审核的有效性。

11.3.2 评估

评价机构评估资格审核效果，主要应包括：

a）受理过程、审核过程的规范性、科学性及对审核效果的影响；

b）受理人员专业素养对审核效果的影响；

c）审核结论的符合性、科学性和权威性及对审核效果的影响等。

12 过程改进

应参照DB21/T 2702.1 第14章、DB21/T 2702.2 第12章，采用PDCA过程方法改进、完善资格审核过程。