ICS 35.020
L 70

DB21

辽　宁　省　地　方　标　准

DB21/T 2702.1—2016

信息安全 个人信息安全管理体系评价 第1部分：要求

Information Security-Personal Information security management system evaluation-Part 1-Requirements

2016－09－27 发布　　2016－11－27 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　要求
——信息安全　个人信息安全管理体系评价　评价管理指南
——信息安全　个人信息安全管理体系评价　评价员管理
——信息安全　个人信息安全管理体系评价　评价指标
——信息安全　个人信息安全管理体系评价　评价方法
——信息安全　个人信息安全管理体系评价　资格审查
——信息安全　个人信息安全管理体系评价　现场管理
——信息安全　个人信息安全管理体系评价　保证方法
——信息安全　个人信息安全管理体系评价　仲裁指南
——信息安全　个人信息安全管理体系评价　审批指南
——信息安全　个人信息安全管理体系评价　资格管理

本部分是 DB21/T 2702 的第 1 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、孙毅、吕蕾蕾、杨莉、司丹、郭玉梅、杨万清、王小更、宋悦。

引　言

0.1　综述

个人信息管理是基于特定、明确、合法目的，以有效、能动、可控、安全为目的、针对个人信息及相关资源、环境、管理体系等的相关活动或行为。

DB21/T 1628系列标准，定义了保证个人信息安全的基本规则和行为准则，约束了个人信息拥有者的管理个人信息的活动和行为。然而，个人信息管理的标准符合性、一致性和目的有效性，必须经第三方认证机构确认。

个人信息安全管理体系评价标准体系，规定了个人信息安全管理体系的认证规则，及个人信息安全管理体系评价机构的行为准则。

0.2　评价

评价是认证的一种形式。个人信息安全管理体系评价，是以个人信息安全为目的，采用合理、有效的技术和管理方法，系统、客观、全面地监督、判断、评估个人信息安全管理体系的建立、实施、完善、变化及其影响因素。

0.3　评价对象

个人信息管理是个人信息管理者向个人信息主体提供服务的过程，通过计划、组织、协调个人信息资源需求与个人信息主体的符合性，采取相应的规范化、系列化控制策略和控制措施，保证个人信息的安全。

相对于组织形态，个人信息管理是发散的。构建个人信息安全管理体系，映射个人信息管理的特征、属性，约束相关因素，可以相互关联、协调，实现个人信息相对安全的状态。

因而，评价的对象是个人信息安全管理体系。

0.4　评价体系

实施个人信息安全管理体系评价的评价体系，是基于个人信息安全目标，整合目标、原则、管理、方法、过程、资源等要素，及实现要素的方法、过程，所形成的知识、方法和实践的有机整体。以保证个人信息安全管理体系评价的科学性、规范性和有效性。

0.5　标准体系

个人信息安全管理体系评价　标准体系包括：

个人信息安全管理体系评价　要求：个人信息安全管理体系评价的基本规则；

个人信息安全管理体系评价　评价管理指南：个人信息安全管理体系评价的实施细则；

个人信息安全管理体系评价　评价员管理：实施个人信息安全管理体系评价人员的约束规则；

个人信息安全管理体系评价　评价指标：个人信息安全管理体系评价的指标设计、构成；

个人信息安全管理体系评价　评价方法：实施个人信息安全管理体系评价的方法设计和选择；

个人信息安全管理体系评价　资格审查：申请个人信息安全管理体系评价的资格评估；
个人信息安全管理体系评价　现场管理：实施个人信息安全管理体系评价的现场审核规则；
个人信息安全管理体系评价　保证方法：实施个人信息安全管理体系评价的质量保证；
个人信息安全管理体系评价　仲裁指南：个人信息安全管理体系评价的争端解决规则；
个人信息安全管理体系评价　审批指南：个人信息安全管理体系评价结果的判定规则；
个人信息安全管理体系评价　资格管理：通过个人信息安全管理体系评价后的管理规则。

0.6　业务连续性

个人信息安全管理体系评价，应基于各类组织的实际，保证业务、管理运行的连续性。

0.7　要求

本标准基于DB21/T 1628系列个人信息安全标准确立的个人信息安全原则和要求，重点描述和指导个人信息安全管理体系评价规则。

实施个人信息安全管理体系评价，应同时使用DB21/T 1628系列个人信息安全标准和本标准确立的个人信息安全管理体系评价　规则。

0.8　兼容性

个人信息安全管理体系评价标准体系，可与B21/T 1628系列个人信息安全标准、其它国际、国内信息安全标准及相关标准协调一致，并与这些标准相互配合或相互参照、整合实施和运行。

个人信息安全管理体系评价标准体系，易于与其它国际、国内相关认证标准整合实施。

0.9　基准

《信息安全　个人信息安全管理体系评价　要求》应做为个人信息安全管理体系评价的基准，其内容并不一定完全适用各类组织。宜根据组织特点、技术发展、行业应用、市场需求等剪裁、设计，或根据本标准规制延伸使用。

信息安全 个人信息安全管理体系评价 第1部分：要求

1 范围

本标准规定了个人信息安全管理体系评价的管理、指标、流程、准备、申请受理、现场审核、审批和公示、仲裁服务、人员管理、文档管理、过程管理和资格管理等的规范。

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实施指南

3 术语、定义和缩略语

3.1 术语和定义

DB21/T 1628界定的以及下列术语和定义适用于本文件。

3.1.1

个人信息安全管理体系评价 personal information security management system evaluate

由独立、公正的第三方评价机构，基于DB21/T1628系列标准，系统、全面、客观地审查、判断、评估个人信息安全管理体系评价实施、运行状况的标准符合性、一致性和目的有效性的活动。

注1：包括自动或非自动处理全部或部分个人信息的个人、企业、事业、社会团体等组织的个人信息管理；

注2：评价与认证是一致的。

3.2 缩略语

3.2.1

PISMSE

个人信息安全管理体系评价。

4 评价管理

4.1 评价原则

4.1.1 以用户为中心

应充分理解用户需求，关注用户业务流程，使评价客观、全面、整体、有效。

4.1.2 基于事实管理

应保证获得数据、信息的可靠性、准确性，基于事实科学、客观分析、判断、评估。

4.1.3 质量管理

应采用PDCA过程管理模式，保证评价质量和评价的权威性。

4.1.4 持续改进

应不断改进、完善评价体系，提高评价体系的有效性，以更加适应用户、社会的需要。

4.2 评价组织

4.2.1 要求

实施PISMSE，应建立相应的管理机构，以约束评价活动、行为。

4.2.2 工作委员会

4.2.2.1 构成

个人信息安全工作委员会是为推进个人信息安全、实施PISMSE设立的专门的管理机构。

a）委员会应由主管机构、相关行业、相关企业代表，及专家、学者和相关研究人员组成；

b）委员会应设立若干职能单元，履行委员会的各项职能，如法规组、仲裁组、宣传组、国际交流组、教育培训组等。

4.2.2.2 职能

个人信息安全工作委员会的职能，主要应包括：

a）推进、实施个人信息安全相关工作；

b）推进PISMS建设；

c）研究、制定、解释、修改、实施个人信息安全相关法规、标准；

d）研究、制定、解释、修改、实施PISMSE相关标准、规则；

e）监督PISMSE机构的工作；

f）审计PISMSE相关活动和文档；

g）推进个人信息安全、PISMSE相关宣传、培训、教育；

h）建立争端解决仲裁机制；

i）国际间的交流、合作等。

4.2.3 评价机构

4.2.3.1 构成

PISMSE机构是个人信息安全工作委员会为管理、实施PISMSE派出的专门机构。

a）评价机构的构成应包括专家、学者、专业人士和管理人员等；

b）评价机构应设立常设机构，如评价办公室。

4.2.3.2 职能

评价机构的职能，主要应包括：

a）评价人员管理

1）评价人员审查、聘任；

2）评价人员培训、考核；

3）评价人员职责和义务；

4）评价人员派出和管理；

5）评价人员相关事务管理；

b）评价事务管理

1）接受PISMSE申请；

2）审查PISMSE资格；

3）审核申请PISMSE提交资料；

4）现场审核PISMS；

5）提交PISMSE相关文档；

6）PISMS复审；

7）发放PISMSE证书；

8）其它PISMSE事务；

c）评价质量控制

1）评价人员评估；

2）评价过程评估；

3）评价效果评估；

4）其它质量相关因素评估；

d）仲裁服务

1）制定投诉处理规则；

2）建立投诉处理流程；

3）建立投诉受理和反馈机制；

4）明确投诉处理人员的职责和义务；

5）建立投诉监督机制；

6）特殊情况处理等；

e）培训教育

1）制订培训教育计划；

2）确定培训教育方式、方法；

3）选择适宜的培训教育教材；

4）明确培训教育师资及相应的职责和义务；

5）培训教育考核；

6）培训教育效果评估；

f）文档管理

1）编制PISMSE资格审核报告；

2）编制PISMSE现场审核报告；

3）编制PISMSE报告；

4）编制PISMSE整改报告；

5）建立PISMSE相关文档管理制度；

6）其它PISMSE相关文档的管理；

g）日常事务管理

1）建立评价机构管理制度；

2）日常事务处理；

3）受理PISMSE相关投诉；

4）其它PISMSE相关事务。

4.3 评价体系

为保证PISMSE的质量，应建立相应的评价体系。评价体系主要应包括：

a）评价对象和评价目的；

b）评价机构管理；

c）评价人员管理；

d）评价方法和手段；

e）评价指标；

f）评价流程；

g）评价过程管理；

h）评价质量管理；

i）评价结果管理等。

5 评价指标

5.1 要求

PISMSE机构应依据DB21/T 1628系列标准，基于不同的个人信息管理者的特征，设计并建立PISMSE的指标体系，以保证PISMSE的科学性、规范性。

5.2 设计

5.2.1 要求

PISMSE指标设计，应考虑：

a）应全面、整体评估、判断PISMS、体系内各个功能要素之间的关联关系；

b）应合理设计评价指标，关注评价指标之间、评价指标项之间的关联关系，避免雷同、重复、矛盾；

c）应基于个人信息管理者的实际，真实、客观、准确地反映个人信息管理者的个人信息安全状况。

5.2.2 结构

PISMSE指标结构，应包括：

a）应基于DB21/T 1628系列标准，设计评价指标整体框架，由通用的PISMSE指标构成；

b）应基于个人信息管理者的实际，设计PISMSE指标的指标项；
c）应根据个人信息管理者的特殊需求设计PISMSE指标和相应的指标项。

5.2.3 构成

PISMSE指标构成参见附录B。

5.3 评估

应在PISMSE的全生命周期评估PISMSE指标的科学性、合理性、可用性和有效性，随时修正、完善PISMSE 指标体系，并持续改进。

6 评价流程

评价流程宜参照附录A设置。

7 评价准备

7.1.1 管理体系

管理体系建立应按照如下要求：
a）个人信息管理者应依据DB21/T 1628.1，建立PISMS，在法规、标准框架内实施个人信息管理；
b）个人信息管理者应依据DB21/T 1628，展开个人信息安全管理体系内审，持续改进、完善PISMS。

7.1.2 自我评价

个人信息管理者应在PISMS运行3个月后实施PISMS自我评价：
a）依据DB21/T 1628系列标准，检查、评估PISMS实施、运行状况；
b）依据DB21/T 1628系列标准，评估PISMS内审结果；
c）依据相关法规、标准，评估PISMS与业务需求的融合度；
d）判断、评估个人信息管理与相关法规、标准的符合性、一致性和有效性；
e）PISMS缺陷整改措施和有效性；
f）申请PISMSE的可行性等。

7.1.3 申报准备

个人信息管理者申请PISMSE，应根据评价机构要求准备相应的资格审核材料：
a）PISMSE申请；
b）个人信息管理者基本情况说明；
c）个人信息管理说明；
d）PISMS实施、运行情况说明；
e）PISMS相关文档；
f）PISMS自我评价报告；
g）其它需要说明的问题等。

8 申请受理

8.1 资格审核

8.1.1 要求

PISMSE机构受理PISMSE申请，应审核申请者的资格。资格审核应包括资格审查和文档审查。

8.1.2 资格审查

评价机构应依据个人信息安全相关法规、标准和其它相关法规、标准，审核申请PISMSE的个人信息管理者的申请资格。审查内容主要应包括：

a）个人信息管理者的合法性；

b）个人信息管理者的业务相关性；

c）PISMS相关文档的规范性、完整性，应包含：

1）个人信息管理相关文档；

2）PISMS自我评价报告；

3）PISMS运行状况评估；

4）PISMS整改措施和相关报告；

5）个人信息安全事故报告；

6）其它需要提供的文档。

d）其它需说明的问题。

8.1.3 文档审查

8.1.3.1 审查条件

评价机构应依据个人信息安全相关法规、标准和其它相关法规、标准，审查申请PISMSE的个人信息管理者提交的PISMS相关文档。审核者应符合条件：

a）审核应由评价机构聘请的相关专业评价人员实施；

b）审核前应明确审核人员的职责和要求；

c）申请评价的个人信息管理者与审核人员无直接关系；

d）应制定审核控制要求和记录要求。

8.1.3.2 审查内容

文档审查的主要内容，应包括：

a）应评估PISMS相关文档的真实性、有效性；

b）应评估PISMS相关文档内容的规范性、完整性；

c）应根据文档初步评估PISMS实施、运行状况；

d）应评估个人信息管理与个人信息安全相关标准、法规的符合性；

e）应评估个人信息管理的有效性；

f）应质疑可能存在的问题，并明确结果。

8.2 审核结论

8.2.1 审核合格

资格审核满足下列条件的，应予合格：

a）PISMS相关文档规范、完整、真实、有效；

b）PISMS实施、运行状况良好；
c）个人信息管理有效，符合个人信息安全相关标准、法规；
d）PISMS运行存在可接受的非实质性问题。

8.2.2 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）PISMS相关文档存在缺陷，需要改进、完善；
b）PISMS实施、运行存在某些需要改进、完善的问题；
c）存在某些需要现场评价确认的一般性问题。

8.2.3 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）PISMS相关文档存在重大隐患（如虚报、瞒报等）；
b）PISMS实施、运行存在重大缺陷；
c）发生重大个人信息安全事故，且
1）事故等级较高；
2）事故处理措施不当；
3）尚在恢复期。

8.3 审核报告

评价机构完成资格、文档审查后，应编制资格审核报告，主要内容包括：
a）个人信息管理者基本情况审查说明；
b）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）不符合、不满足PISMSE　要求事项说明；
f）符合基本合格要求的个人信息管理者出具的整改报告；
g）审核结论等。

9 现场审核

9.1 审核组织

9.1.1 审核组

资格审核合格后，评价机构应组建PISMSE现场审核组，实地判断、评估个人信息管理者PISMS实施、运行状况。

9.1.2 审核计划

现场审核组组长应根据资格审核报告、个人信息管理者实际和相关法规、标准等编制PISMSE现场审核计划：
a）个人信息管理者基本信息；
b）资格审查报告说明；

c）现场审核组的职能、职责；
d）PISMSE现场审核重点；
e）PISMSE现场审核方法；
f）PISMSE现场审核有效性验证；
g）PISMSE现场审核安全性保证；
h）PISMSE现场审核文档管理等。

9.2 审核会议

9.2.1 要求

在PISMSE现场审核中，审核组应以会议的形式完成现场审核准备，及审核组内部、审核组与个人信息管理者之间的沟通、交流、说明等。

9.2.2 审核准备

审核组应在进入现场前召开全体审核人员会议，说明PISMSE现场审核计划，明确PISMSE现场审核的目的和任务。

9.2.3 进入现场

审核组应在进入现场后召开由审核人员和个人信息管理者与个人信息安全相关责任人参加的工作会议。会议内容应包括：
a）依据个人信息安全相关法规、标准，说明PISMSE的目的；
b）说明PISMSE现场审核计划；
c）说明PISMSE现场审核要求；
d）说明PISMS原始文档收集要求；
e）说明PISMSE现场审核抽样方法；
f）确认PISMSE现场审核所需资源；
g）澄清可能存在的问题；
h）个人信息管理者准备情况说明。

9.2.4 审核过程

审核组应在PISMSE现场审核过程中适时召开工作例会，会议内容应包括：
a）及时通报、沟通、交流现场审核信息；
b）及时研究、讨论现场审核中无法确认、含糊不清等问题；
c）应形成一致、统一的结论。

9.2.5 审核结束

审核组应在现场审核结束后召开由审核人员和个人信息管理者与个人信息安全相关责任人参加的工作会议，会议内容应包括：
a）依据个人信息安全相关法规、标准，说明PISMSE的目的；
b）说明PISMSE现场审核计划执行情况；
c）说明PISMSE现场审核抽样方法；
d）解释、说明PISMSE现场审核发现的问题；
e）个人信息管理者应澄清或确认审核组提出的问题；

f）PISMS实施、运行状况判断、评估说明；

g）明确说明PISMSE现场审核意见；

h）说明PISMS修正、完善、改进要求和建议；

i）说明PISMSE现场审核意见存在疑义的申诉过程；

j）说明PISMSE现场审核事后监督程序等。

9.3 调查方法

9.3.1 面谈

现场审核人员应根据现场审核准备阶段确定的审核目标、审核内容及资格审查中需要确认的问题，设计面谈样本，并依据样本分别访问相关人员。面谈方式可包括：

a）集体面谈：与PISMS相关责任人集体访谈，调查并确认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，调查个人对个人信息安全的理解和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PISMS对客户的影响等。

注：面谈应与其它调查方法结合使用。

9.3.2 文档检查

审核组应依据DB21/T1628.2，检查个人信息管理相关文档、PISMS相关文档的原始纪录和资料，调查并确认个人信息管理机制的状况。

9.3.3 抽样调查

8.3.3.1 要求

审核组应根据面谈、文档检查结果，选取适宜的样本，调查PISMS实施、运行状况。

8.3.3.2 样本选择

选择抽查样本，应考虑：

a）业务流程：应选择典型的、与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个人信息管理、处理、使用环节；

d）异常现象：应选择PISMSE过程中存在疑问或异常的事件等。

8.3.3.3 抽样范围

抽样范围应满足如下要求：

a）抽样范围应包括时间范围、样本选择范围、样本检查范围等；

b）抽样范围应依据个人信息安全相关法规和标准、PISMS现场审核计划和个人信息管理者的实际，以及PISMS实施、运行状况确定。

8.3.3.4 抽样数量

抽样数量应保证抽查样本可以反映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。确定抽样数量，一般考虑：

a）规模：抽样数量可根据个人信息管理者的规模确定；

b）实际状况：应根据个人信息管理的重视程度、PISMS实施运行的有效性确定；

c）缺陷：应根据个人信息管理和PISMS实施运行的缺陷和薄弱环节确定。

8.3.3.5 抽查结论

抽样调查结束后，应形成抽样调查结论。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，应根据个人信息安全相关法规、标准形成。

9.4 审核实施

9.4.1 要求

现场审核实施要求包括：

a）现场审核人员要求：

1）现场审核人员应科学、专业、客观地分析、判断、评估PISMS运行状况；

2）现场审核人员不应根据个人好恶主管臆断，有悖事实；

3）现场审核人员应从全局角度综合判断、评估分工范围内的个人信息管理状况；

b）调查样本人员要求：

接受调查的样本人员应真实、客观地说明相关问题，避免自身利益考虑或忽视事实的情况。

9.4.2 审核质量

9.4.2.1 要求

应在PISMSE现场审核中实施质量控制，避免和减少调查偏差，以真实反映个人信息管理者的个人信息安全状况。

9.4.2.2 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）应符合个人信息安全相关法规、标准和个人小信息管理者的实际；

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，并说明个人信息管理现状、缺陷、漏洞、隐患和影响等。

9.4.2.3 问题处理

在现场审核过程中，应及时处理影响PISMSE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。

9.4.3 调查偏差

在现场调查中，应注意偏差控制，避免或减少各种原因引起的偏差：

a）偏差类型：

1）整体偏差：在现场审核的广告环节均可能出现的偏差；

2）随机偏差：在抽样调查中可能出现的偏差；

b）偏差原因：可能造成偏差的原因包括：

1）面谈提问；

2）审核双方的心理状态；

3）调查文档的设计质量和填写质量；

4）调查分析的主观因素；

5）抽查样本的选择；

6）沟通、交流不充分等。

9.4.4 沟通交流

在现场审核过程中，应与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。

9.5 审核结论

9.5.1 要求

PISMSE现场审核结束后，现场审核组应整理、分析、判断、评估现场调查中累积的所有相关信息，清楚、明确地说明个人信息管理的问题，形成客观、真实、公正的审核意见。

9.5.2 问题分类

现场审核中发现的问题，主要应分为2大类：

a）严重问题：以下问题应视为严重问题：

1）实际情况与申报资料不符（隐瞒事实、虚报、瞒报等）；

2）存在严重的个人信息安全隐患（或经整改后仍不能达到个人信息安全要求）；

3）出现严重的个人信息安全事故等；

b）一般问题：以下问题应视为一般问题：

1）因未充分理解PISMSE要求出现的申报资料不规范、内容不完整等情况；

2）存在一般性的个人信息安全隐患，经整改可在短期内达到个人信息安全要求；

3）其它非实质性问题。

9.5.3 审核意见

现场审核意见应分为2种：

a）通过现场审核：

1）个人信息管理严谨、规范，个人信息安全管理体系实施、运行安全、可靠，符合个人信息安全相关法规、标准和PISMSE要求，满足个人信息主体的个人信息安全需求；

2）存在少量一般性问题，经简单改进、修正，可基本符合个人信息安全相关法规、标准和PISMSE要求，满足个人信息主体的个人信息安全需求；

3）存在短期内可修改、纠正的非实质问题，应经整改后再次申请现场审核，如基本符合个人信息安全相关法规、标准和PISMSE要求，满足个人信息主体的个人信息安全需求，且问题已经修正；

b）不通过现场审核：

1）存在短期内可修改、纠正的非实质问题，但经过整改仍不能达到个人信息安全相关法规、标准和PISMSE　要求；

2）存在严重问题，不符合个人信息安全相关法规、标准和PISMSE　要求，完全不能满足个人信息主体的个人信息安全需求。

9.6　整改

9.6.1　整改意见

现场审核组应以工作例会的形式，分析、研究、判断、评估问题存在的根本原因，确定问题的性质和分类，形成一致的、符合事实的整改意见，并提出适合的改进措施和解决方案。

9.6.2　整改报告

现场审核完成后，存在9.5.3 a）2）、3）问题的个人信息管理者，应在问题解决后形成整改报告，主要内容应包括：

a）问题说明；

b）整改措施和方法；

c）内审报告；

d）自评结果和说明；

e）其它需说明的事项。

9.7　现场审核报告

PISMSE现场审核完成后，应形成现场审核报告，主要内容应包括：

a）个人信息管理者情况说明；

b）PISMS实施、运行状况；

c）现场审核过程说明；

d）问题说明和分析；

e）现场审核结论和说明；

f）建议和意见等。

10　审批和公示

10.1　审核

PISMSE现场审核结束后，现场审核组应将资格审核报告、现场审核报告等PISMSE相关文档提交评价机构审核，审核内容主要应包括：

a）PISMSE是否符合个人信息安全相关法规、标准；
b）PISMSE依据是否充分、有效；
c）PISMSE方法是否适当、合理；
d）现场审核中收集的信息是否典型、齐全；
e）资格审核、现场审核结论是否适当、正确；
f）文字描述是否准确等。

10.2 评价报告

评价机构审核通过后，应由现场审核组编制PISMSE报告。评价报告内容主要应包括：
a）个人信息管理者情况说明；
b）资格审核报告说明；
c）现场审核报告说明；
d）整改报告说明；
e）评价结论认定和说明；
f）评价分析说明等。

10.3 审批

评价报告完成后，应报个人信息安全工作委员会审批，并签署审批意见。如未通过审批，个人信息管理者应整改后重新申请现场审核。

10.4 公示

PISMSE通过审批后，应通过适当方式公示：
a）如公示期内无重大投诉、质疑，应正式通过PISMSE，并发布公告；
b）如公示期内出现重大投诉、质疑，且经证实，应取消相应的PISMSE申请资格，并经整改后重新申请。

11 仲裁服务

评价机构应提供仲裁服务，处理PISMSE相关的投诉、意见、建议和相应的反馈。主要应包括：
a）制定投诉处理规则；
b）建立投诉处理流程；
c）明确投诉受理人的职责和义务；
d）建立投诉受理和反馈机制；
e）建立意见和建议的受理和反馈机制；
f）建立监督机制；
g）建立特殊情况处理机制；
h）其它必须的事项。

12 人员管理

12.1 要求

评价机构应建立PISMSE人员的管理机制，以保证PISMSE的质量、专业、效果。

12.2 构成

PISMSE人员应包括IT、信息安全、管理等相关领域及相关行业或领域的专家、学者、专业技术人员和社会人士。

12.3 资格

PISMSE人员，应根据业务能力、专业能力和从业经验等划分不同的评价资格等级，并明确相应的评价能力。

12.4 制度

评价机构应建立PISMSE人员管理制度，以保证PISMSE的权威性、独立性。主要应包括：

a）资格认定；

b）职责和义务；

c）行为规范；

d）资格等级等等。

12.5 培训

12.5.1 计划

评价机构应根据不同评价资格等级的评价人员能力要求制定相应的PISMSE相关的培训教育计划。

12.5.2 内容

评价机构实施评价人员相关知识培训，主要应包括：

a）个人信息安全相关法规、标准；

b）个人信息安全相关知识；

c）PISMS相关知识；

d）PISMSE 的基本知识；

e）PISMSE 基本方法等。

12.5.3 方式

PISMSE培训教育，宜采用2种培训方式：

a）定期：

1）根据培训教育计划定期实施；

2）根据PISMSE过程中的问题定期、实时实施；

b）研讨：

1）评议PISMSE过程；

2）针对典型案例、有争议问题，或设定课题讨论。

13 文档管理

13.1 记录

应在PISMSE过程中记录所有与评价活动和行为相关的信息，包括目的、依据、时间、对象、人员、方式方法、和过程等。

13.2 文档

应在PISMSE过程的各个阶段形成相应的文档，包括计划、大纲、表格、报告等。

13.3 备案

应建立与PISMSE相关的记录、文档、规章、文件、合同等的备案管理制度，并应根据实际需要改进和完善。

14 过程管理

14.1 过程模式

应在PISMSE过程中分析、发现PISMSE流程存在的缺陷，并采用PDCA模式，修正、改进。

14.2 持续改进

应通过过程管理，分析PISMSE目标、结果、过程和相关资料，发现PISMSE的体系缺陷，持续改进，以提高PISMSE的有效性。

15 资格管理

15.1.1 要求

a）通过PISMSE的个人信息管理者，应履行个人信息管理的职责和义务，基于PDCA模式，持续改进、完善PISMS，保障个人信息主体权益；

b）评价机构应审计、监督、管理通过PISMSE的个人信息管理者，定期复查、复审，以保证评价效果的持续性、实效性。

15.1.2 复查

评价机构应定期抽查通过PISMSE的个人信息管理者，并监督抽查不合格的个人信息管理者整改：

a）合格：个人信息管理工作持续、有效，PISMS运行安全、可靠，且持续改进、完善；

b）不合格：个人信息管理者通过PISMSE后，个人信息管理工作停滞，PISMS不能持续改进、完善，个人信息主体权益存在安全风险，应限期整改；

c）整改后不合格：抽查不合格的个人信息管理者，限期整改后仍不能满足个人信息安全相关法规、标准和PISMSE要求，则应取消相应的PISMSE申请资格，并限定整改周期，经整改后重新申请。

15.1.3 复审

个人信息管理者通过PISMSE后，评价机构应根据不同情况复审：

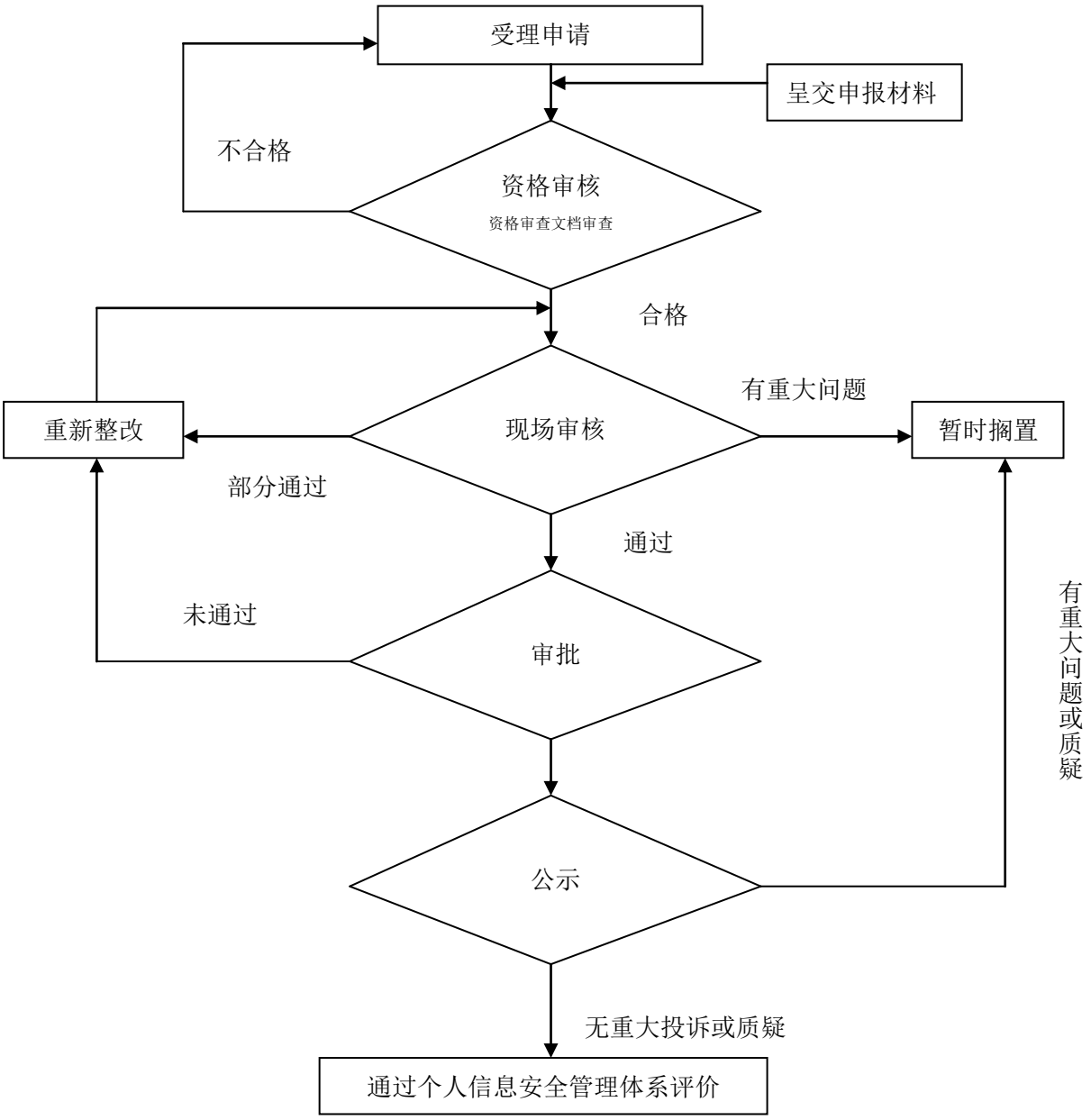
a）应在通过PISMSE后定期复审；

b）个人信息管理者更名、法人变更、义务变化、办公场所更换等，应重新申请现场审核；

c）个人信息管理者通过PISMSE后，出现个人信息安全重大事故，应通过复审确认，取消相应的PISMSE申请资格，并限定整改周期，经整改后重新申请；

d）个人信息管理者通过PISMSE后，评价机构接到投诉，质疑个人信息管理的重大失误、缺陷等，应通过复审确认，取消相应的PISMSE申请资格，并限定整改周期，经整改后重新申请。

附 录 A
（规范性附录）
评价流程



附 录 B
（规范性附录）
评价指标构成

PISMSE 指标构成：

$$es=\{et_1(ei_1,\ldots\ldots ei_n)\ ,\ et_2(ei_1,\ldots\ldots ei_n),\ldots\ldots et_m\ (ei_1,\ldots\ldots ei_n)\}$$

其中 es ——评价指标体系

et——评价指标

ei——评价指标项

$ei=\{ec_1，ec_2，\ldots\ldots ec_n\}$

ec——指标子项

m，n=1，2，……