ICS 35.020
L70

DB21

辽　宁　省　地　方　标　准

DB21/T 2702.2—2018

信息安全 个人信息安全管理体系评价 第2部分：管理指南

Information security-Personal information security management system evaluation-Part2: Management guidelines

2018－01－22 发布　　2018－02－22 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 2 部分。

本部分按照 GB/T 1.1—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。

本部分由大连市质量技术监督局提出。

本部分由辽宁省工业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、大连市计算机学会。

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2部分：管理指南

1 范围

本标准为构建个人信息安全管理体系评价的评价体系、评价管理、评价规则，及个人信息安全管理体系评价实施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

3 术语和定义

DB21/T 1628、DB21/T 2702.1 界定的以及下列术语和定义适用于本文件。

3.1

评价 evaluation

事物的分析、判断和评估。

3.2

主体 principal part

具有法人资格并承担相应责任和义务的组织机构。

3.3

评价主体 evaluation of principal part

依法取得法人资格并具有相应资质，获得个人信息管理机构认可，独立从事PISMSE活动的机构。

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 PISMSE 的管理和实施。

管理、实施 PISMSE，应以 DB21/T 1628 系列标准为基准。

管理、实施 PISMSE，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。

管理、实施PISMSE，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

5.1 相关方

5.1.1 第一方

PISMSE的第一方应是个人信息管理者。

a）个人信息管理者应通过内审和过程管理，保证PISMS的有效、安全和可靠，提高个人信息管理者的信用保证；

b）个人信息管理者应遵循DB21/T 1628.2 9的规则；

c）个人信息管理者应获得评价主体的评价认可。

5.1.2 第二方

PISMSE的第二方应是个人信息主体。

a）个人信息管理者管理个人信息的合理、有效、充分，及个人信息主体权益的保障，应由权威、有信誉的评价主体提供保证；

b）个人信息主体的权力和义务应遵循DB21/T 1628.1 5、DB21/T 1628.2 7的规则；

c）个人信息主体应通过PISMSE认知个人信息管理者的管理能力和服务质量。

5.1.3 第三方

5.1.3.1 主体

PISMSE的第三方应是评价机构，是从事PISMSE的评价主体，应包括以下特征：

a）合法、有效、独立并具有相应资质的法人组织；

b）独立行使法定权力，承担社会责任和法律义务；

c）获得管理机构的认可；

d）有固定的工作环境和必要的相关设备、设施等及相应的技术能力；

e）依据DB21/T 2702.1 4.2.3，具备评价机构职能和相应的管理制度、管理机制；

f）具有DB21/T 2702.1 12规定的评价人员规则和相应的管理制度、管理机制；

g）评价机构的最高管理者、各级责任主体应具备履行PISMSE必备的知识、能力、责任、义务等；

h）具有取得评价能力认定的专职高、中、低级评价人员配备；

i）依据个人信息安全相关法规、标准应具备的其它条件。

5.1.3.2 责任和义务

5.1.3.2.1 责任

评价主体应承担的责任主要包括：

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。

5.1.3.2.2 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。

5.2 对象

5.2.1 个人信息管理者

个人信息管理者是个人信息的管理主体，应遵循DB21/T 1628.1第6章和DB21/T 1628.2第9章的规定，以保证个人信息管理的安全、规范、有效。

5.2.2 个人信息管理

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，应遵循DB21/T 1628.1和DB21/T 1628.2的约束规则，保证个人信息安全。

5.2.3 PISMS

PISMS应是PISMSE的对象，其主要特征应包括：
a）个人信息管理者的基本状态；
b）个人信息管理的特征、属性；
c）个人信息管理的策略、机制；
d）个人信息管理的过程、质量控制；
e）个人信息管理的安全风险评估等。

6 评价管理

6.1 概述

6.1.1 要求

DB21/T 2702.1第4章确立了PISMSE的基本规则，评价主体应符合DB21/T 2702.1 4.2.3的规定，并应基于DB21/T 1628系列标准，依据DB21/T 2702.1和本标准实施PISMSE。

6.1.2 原则

评价主体应遵循DB21/T 2702.1 4.1确立的PISMSE的基本原则，并在评价中细化、明确原则实施的细节，保证PISMSE的客观性、有效性和充分性。

6.2 评价边界

依据DB21/T 2702.1，评价主体应确定PISMSE的边界，主要应包括：

a）范围和特征：个人信息的分布范围和存在特征；

b）层级和权责：个人信息管理者内部管理、业务层次和权限、责任及与PISMS的关系；

c）部门间：个人信息管理者内部各部门之间的关联、影响及与PISMS的关系；

d）外部：个人信息管理者与客户、社会组织之间的关联、影响及对PISMS的影响；

e）责任主体：与个人信息相关责任主体的职能、职责、权限；

f）体系设计：PISMS的层级及权责设计；

g）业务关系：PISMS与业务连续性的关系；

h）变化：个人信息管理者内部管理、业务发生变化对PISMS的影响；

i）个人：个人信息管理者的员工、PISMS相关人员的行为、责任等。

6.3 评价组织

6.3.1 要求

评价组织应考虑：

a）DB21/T 2702.1 4.2确立的评价组织规则，应是PISMSE的组织保障，应首先依据DB21/T 2702.1 4.2组建；

b）管理机构应依据DB21/T 2702.1 4.2设置PISMSE管理的相关职能单元，以保证PISMSE的规范性、科学性；

c）评价主体应在PISMSE全生命周期实施符合相关法规、标准的管理，组织PISMSE相关活动。

6.3.2 管理主体

应首先明确评价管理机构的管理主体，并在管理主体的支持、指导下开展PISMSE活动。管理主体的职责主要应包括：

a）理解个人信息安全，明确PISMSE的目的；

b）提供利于PISMSE的管理平台，积极推进PISMSE；

c）组建相应的管理机构，遴选具有相应知识、能力、专业等的管理人员，保证PISMSE的实施；

d）为推进、实施PISMSE提供所需资源支持，包括人员、资金、信息、管理、环境等；

e）对PISMSE管理过程中可能出现的各种不利因素提供管理决策；

f）对PISMSE管理和PISMSE提供指导和决策；

g）批准PISMSE管理机构的组建、职责分配及相应的管理机制等。

6.3.3 管理机构

6.3.3.1 要求

管理主体应依据DB21/T 2702.1 4.2指导、批准设立PISMSE管理机构：

a）依据DB21/T 2702.1 4.2.2，机构名称宜称为个人信息安全工作委员会；

b）依据DB21/T 2702.1 4.2.2.1，管理机构的构成应具有广泛的代表性，不应局限于某一领域或行业；

c）依据DB21/T 2702.1 4.2.2.1，管理机构应根据PISMSE的特征和功能属性，设立若干职能单元，分工负责，共同履行管理机构的职能。

6.3.3.2 管理

管理机构应依据DB21/T 2702.1 4.2.2，建立管理机制：

a）应明确工作章程，确定管理机构的目标；

b）应依据工作章程建立相应的工作机制、管理流程；
c）应明确各项职能，参看DB21/T 2702.1 4.2.2.2；
d）应明确管理机构成员的产生机制、工作职责等。

6.3.3.3 职能单元

依据DB21/T 2702.1 4.2.2.1，管理机构宜设立若干职能单元，宜包括：
a）法规组：法规组的职能应包括：
1）个人信息安全相关法规、标准、制度的研制；
2）个人信息安全相关法规、标准、制度的相关理论和实践研究、解释；
3）PISMSE相关规则、标准研制、审核；
4）PISMSE相关规则、标准的相关理论和实践研究、解释；
5）PISMS建设咨询、指导等；
b）仲裁组：仲裁组的职能应包括：
1）个人信息安全事件、事故的认定、说明；
2）个人信息安全事件、事故的处理、说明；
3）个人信息管理与个人信息主体之间的问题处理、说明；
4）PISMSE相关投诉、质疑的处理、说明；
5）个人信息安全相关问题咨询、指导等；
c）宣传组：宣传组的职能应包括：
1）理解、阐释个人信息安全相关法规、标准；
2）理解、阐释PISMSE相关规则、标准；
3）个人信息安全相关法规、标准、制度的宣贯、推广；
4）PISMSE相关规则、标准的宣贯、推广；
5）个人信息安全相关知识、实践的阐述、说明；
6）PISMS相关知识、实践的阐述、说明；
7）PISMSE相关知识、实践的阐述、说明；
8）个人信息管理相关问题咨询、说明等；
d）国际交流组：国际交流组的职能应包括：
1）个人信息安全相关法规、标准、制度的解释、说明；
2）PISMSE相关规则、标准的解释、说明；
3）个人信息安全相关法规、标准、制度的相关理论和实践研究的说明；
4）PISMSE相关规则、标准的相关理论和实践研究说明；
5）国际间的交流、合作；
6）中国个人信息安全相关问题的咨询、解释、说明等；
e）教育培训组：教育培训组的职能应包括：
1）面向社会：
•个人信息安全基础理论、实践教育、培训；
•个人信息安全相关法规、标准、制度的解读、培训；
•PISMSE相关规则、标准的解读、培训；
•PISMS实训教育、培训等；
2）面向内部：
•个人信息安全基本知识；
•PISMSE基本知识；

•个人信息安全相关法规、标准、制度；
•PISMSE基本知识、规则、标准；
•PISMS实训；
•评价人员基本技能；
•评价人员基本素质等。

6.3.4 评价机构

6.3.4.1 要求

依据DB21/T 2702.1 4.2.3，评价机构应是管理机构为管理、实施PISMSE派出的评价主体：
a）依据DB21/T 2702.1 4.2.3.1，评价机构的组成应具有权威性、代表性；
b）依据DB21/T 2702.1 4.2.3.1，评价机构应设立常设机构，处理日常事务、管理评价相关事宜。

6.3.4.2 管理

评价机构应依据DB21/T 2702.1 4.2.3，建立相应的管理机制：
a）应建立评价机构管理制度和相应的实施细则；
b）应建立评价机构工作流程、评价管理机制；
c）应明确评价机构各项管理职能；
d）应明确评价管理人员的职责和义务等。

6.3.4.3 工作流程

评价机构应建立工作流程，参看附录A。

6.3.4.4 职责

评价机构应明确管理职责，主要应包括：
a）PISMSE的前期咨询、解释；
b）个人信息安全相关法规、标准的解释、说明；
c）PISMSE相关规则、标准的解释、说明；
d）PISMS建设指导、咨询；
e）受理PISMSE申请；
f）审查PISMSE申请资格；
g）评价人员聘用、管理；
h）PISMSE现场审核组组建、管理；
i）PISMSE相关文档管理；
j）评价结论、评价资格管理；
k）投诉、建议和反馈管理等。

6.3.4.5 管理制度

应建立评价机构管理的相关规章制度，主要应包括：
a）评价机构的构成和职责；
b）评价机构服务准则；
c）评价机构工作流程；
d）评价事务管理；

e）安全保密规定；
f）相关文档管理；
g）罚则；
h）其它必要的制度等。

6.4 组织

评价机构应依据个人信息安全相关法规、标准，组织PISMSE相关活动：
a）建立PISMSE体系，保证PISMSE的质量；
b）明确评价管理职责和管理人员行为规范；
c）选择、聘请具有相应能力的评价人员，保证评价的独立性、客观性；
d）实施PISMSE；
e）评估PISMSE质量、效果；
f）PISMSE后管理；
g）其它相关管理。

6.5 控制

评价机构应依据个人信息安全相关法规、标准，检查、修正评价管理相关活动，监督、跟踪PISMSE的实施。

6.6 协调

评价机构在评价管理中，应注意与第一方、评价人员、现场审核组、管理机构等之间的协调、沟通：
a）PISMSE目的的一致性、实施有效性；
b）PISMSE边界的合理性、特征符合性；
c）评价人员的能力、水平和公正性、客观性；
d）评价方法、手段的适宜性、可用性；
e）评价指标的符合性、适用性；
f）评价流程的可用性；
g）评价质量的可控性；
h）评价结果的准确性、客观性、科学性等。

7 评价体系

7.1 评价要素

PISMSE的要素，主要应包括：
a）评价目的：PISMSE应实现的目标；
b）评价主体：评价机构；
c）评价对象：PISMS；
d）评价因素：PISMSE指标体系、指标因子；
e）评价方法：PISMSE规则、各种方法；
f）等级：PISMSE等级标准和划分原则；
g）权重：PISMSE指标的影响度、重要性；
h）评价过程：PISMSE过程管理；

i）评价结果：获得PISMSE的结果；

j）评价效益：评价主体的主客观因素对评价结果的影响和认可等。

7.2 构成

7.2.1 要求

PISMSE体系的构成，应包括评价规则、评价指标和权重。

7.2.2 评价规则

7.2.2.1 内容

PISMSE的规则，主要应包括：

a）确定PISMSE指标；

b）根据个人信息安全相关法规、标准制定评价等级标准；

c）根据等级标准划分评价等级和每个等级的评分范围；

d）确定评价指标子项和对应的分值；

e）根据等级标准对各个评价指标和指标子项评分、加权，计算得分和总分。

7.2.2.2 等级

应根据个人信息安全相关法规、标准划分评价等级，以区分个人信息安全程度。评价等级可划分为4级：

a）1级：在基于个人信息全生命周期的管理中，存在明显的缺陷，PISMS不完善，评价总分较低；

b）2级：在基于个人信息全生命周期的管理中，存在部分缺陷，但PISMS较完善，评价总分一般；

c）3级：在基于个人信息全生命周期的管理中，存在微小缺陷，PISMS完善，评价总分较高；

d）未通过现场审核：在基于个人信息全生命周期的管理中，存在严重缺陷，不能保证个人信息安全和个人信息主体权益。

7.2.2.3 评分范围

应采用百分制，并确定评价等级的取值空间，一般可划分为：

a）1级：评分范围可在25分内；

b）2级：评分范围可在15分内；

c）3级：评分范围可在10分内。

7.2.2.4 权重

应根据PISMSE指标相对于个人信息管理者实际需求的重要性，相互比较确定每个评价指标的权重。

7.2.2.5 加权

各个评价指标累加总分加权计算获得评价总分：

$$E=\sum W_i \times V_i$$

W_i：每个评价指标（i）定义的权重；

V_i：每个评价指标（i）累加的总分。

7.3 构建 PISMSE 体系

评价机构应依据DB21/T 2702.1 4.3组织构建评价体系：

a）明确PISMSE的目的，确立PISMSE的基本原则；

b）确定评价对象，根据评价对象的特征，明确PISMSE的边界和PISMSE的相应资源需求；

c）建立评价机构的管理机制，明确机构职能、管理职责和相关人员的职责；

d）选聘具有相应能力的评价人员，建立相应的评价人员管理机制、培训机制和能力评价机制；

e）基于评价对象的特征，分析、判断评价对象的各种关联因素，选择适宜的评价方法和手段；

f）基于评价对象的特征，设计、建立相应的PISMSE指标体系；

g）基于个人信息管理者的实际和评价规则，确定评价指标的权重；

h）建立科学、规范的评价流程，包括受理申请、资格审核、现场审核、仲裁服务、审批、资格管理等；

i）建立PDCA过程管理模式，在PISMSE实施中，不断修正、改进评价流程，持续改进评价体系；

j）建立评价质量管理体系，通过过程管理，跟踪、监控评价过程；

k）建立评价结果管理机制，保证评价数据、信息可靠，判断、评估科学、客观。

8 评价指标

8.1 概述

8.1.1 要求

依据DB21/T 2702.1 5.1，评价机构组建现场审核组后，应由现场审核组根据个人信息管理者的特征，设计并建立PISMSE指标体系。

8.1.2 指标体系

指标体系应考虑的要素，主要应包括：

a ）个人信息安全相关法规、标准；

b）个人信息安全目标和PISMSE目的；

c）个人信息管理者的组织、管理、业务特征；

d）个人信息管理者的环境（包括工作环境）特征；

e）个人信息管理者内部个人信息的分布、关联因素；

f）个人信息管理活动、行为和变化；

g）PISMS的构建、实施和运行；

h）PISMS内审内容设计和内审结果；

i）资格审核中文档审查结果；

j）个人信息管理者与外部的关联和影响等。

8.2 设计

8.2.1 要求

依据DB21/T 2702.1 5.2.1，PISMSE指标设计应考虑多种因素间的关联关系：

a）整体评价与评价指标：各个评价指标的评估、判断，应是相互关联的，形成PISMS的整体评价；

b）评价指标间：应在设计评价指标时，考虑评价指标之间、评价指标项之间相互关联的整体关系，避免雷同、重复、矛盾和混乱，降低复杂度和评价成本；

c）评价指标项间：应考虑单一指标项的合理性与整体评价中各个指标项的合理性；

d）业务流程与评价指标：应考虑评价指标的客观、全面、系统与业务流程的自由度；

e）管理与执行：应综合判断、评估个人信息管理者内部管理层、执行层等各层级的个人信息管理状况；

f）PISMS：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；

g）评价指标与评价结果：应考虑评价指标与评价结果之间可供选择的评判区间，整体、全面、综合评价PISMS。

8.2.2 结构

依据DB21/T 2702.1 5.2.2，PISMSE指标体系结构，参看附录B。

8.2.3 构成

依据DB21/T 2702.1 5.2.3，PISMSE指标构成示例，参看附录D示例。

8.2.4 评估

应依据DB21/T 2702.1 5.3，评估PISMSE指标体系的科学性、合理性、可用性和有效性，完善并持续改进：

a）指标体系与个人信息安全相关法规、标准的符合性；

b）指标体系与个人信息管理者实际的符合性；

c）评价指标、指标项的合理性、针对性；

d）评价结果与评价指标间的契合度等。

9 过程管理

9.1 要求

PISMSE应依据DB21/T 2702.1 第7章、第8章和第9章的规则，遵循DB21/T 2702.1 第6章确立的流程实施。

9.2 管理机制

PISMSE过程中，应明确相关管理机制：

a）确定PISMSE的目标、方法、策略；

b）确定清晰的质量管理目标；

c）明确管理机构、管理人员和评价人员的职责；

d）保证现场审核组的独立性、公正性和权威性；

e）保证评价人员的业务素养、个人修养、专业水平；

f）确定以评价对象为中心、基于事实管理的原则；

g）保证PISMSE相关文档的严谨、规范、完整；

h）建立PISMSE追踪、评估机制；

i）建立投诉仲裁、意见反馈机制；

j）其它必要的管理机制。

9.3 评价实施

9.3.1 评价机构

评价机构应依据评价工作流程：

a）评价机构的常设机构应依据DB21/T 2702.1 8.1.2审查PISMSE申请者的资格，确认ISMSE申请者具有PISMSE申请资格。

b）确认PISMSE申请者具有PISMSE申请资格后，选聘具有相应能力的评价人员，审查PISMSE申请者提交的PISMSE申报文档。

注1：相应能力，参看 DB21/T 2702.3.

9.3.2 资格审核

9.3.2.1 资格审查

9.3.2.1.1 工作内容

依据DB21/T 2702.1 8.1.2 确立的资格审查内容，评价机构的常设机构的审查，主要应包括：

a）申请条件：

1）申请PISMSE的个人信息管理者的基本状况；

2）PISMSE申请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；

3）申请PISMSE前未发生个人信息安全相关事故、事件；

4）申请PISMSE前存在的个人信息安全隐患、缺陷的有效整改、完善；

5）PISMSE申请者根据实际需求主动申请PISMSE等；

b）文档准备

1）PISMSE申请者基本情况说明；

2）依据DB21/T 1628.1 7，提交个人信息管理相关文档；

3）依据DB21/T 1628.1 8、9、10、11，提交PISMS相关文档；

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

5）PISMS整改、个人信息安全事故等相关报告；

6）.其它需要说明的问题等；

c）申请评估：

1）申请条件评估；

2）申报文档规范性、完整性评估；

d）评估结论：

1）同意受理申请，确认具备PISMSE资格：

- 申报文档规范、完整、真实；
- 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；
- 初步评估个人信息安全隐患、缺陷等得到有效整改、完善；
- 无个人信息安全事故；

2）改进、完善后重新评估，存在以下问题之一：

- 申报文档不完整或不规范；
- 初步评估个人信息管理、PISMS运行存在缺陷；
- 初步评估个人信息安全隐患、缺陷等未得到有效整改；

3）取消申请PISMSE资格：

- 申报文档存在重大隐患（如虚报、瞒报等）；
- 申报文档粗制滥造；
- 存在重大个人信息安全事故等。

9.3.2.1.2 审查方式

资格审查方式主要应包括：

a）面谈：评价机构人员与申请PISMSE的文档提交者面谈，了解PISMSE申请者、评价对象的基本情况；

b）审查文档：根据9.3.2.1.1初步审查PISMSE申请者提交的文档等。

9.3.2.2 文档审查

评价机构选聘的评价人员，应依据DB21/T 2702.1 8.1.3 确立的资格审查规则和内容，审查PISMSE申请者提交申报文档：

a）初步评估PISMSE申请者个人信息管理的有效性和法规、标准的符合性；

b）明确需要整改的问题和需要现场审核确认的问题。

9.3.2.3 整改报告

在资格审查、文档审查中确认需要整改的问题，均应形成整改意见，反馈到PISMSE申请者；

PISMSE申请者应在整改完成后提交整改报告，说明整改措施等。

9.3.2.4 审核结论

审查文档的评价人员，应依据DB21/T 2702.1 8.2、资格审查结论、整改报告，形成资格审核结论，并依据DB21/T 2702.1 8.3编制资格审核报告。

9.3.3 现场审核

9.3.3.1 要求

资格审核确认后，评价机构应依据DB21/T 2702.1 9，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评价人员担任组长：

a）审核组长应明确职责和审核组职能；

b）审核组长应明确PISMSE的目标，并分解目标，分工各位评价人员负责；

c）审核组长应在文档审查中基本了解PISMSE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PISMSE的质量。

9.3.3.2 职责

9.3.3.2.1 审核组长

现场审核组组长职责，主要应包括：

a）负责现场审核组PISMSE各阶段的工作；

b）负责PISMSE管理和质量管控；

c）依据个人信息安全相关法规、标准和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PISMSE现场审核计划，并组织实施；

f）根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）提交PISMSE报告；

k）履行评价人员的职责等。

9.3.3.2.2 评价人员

现场审核组评价人员的职责，主要应包括：

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PISMS构建、实施、运行状况，理解个人信息管理者实际；

d）基于PISMS整体状况，判断、评估分工范围内的PISMS构成要素；

e）与分工范围内的个人信息管理者的相关人员交流、沟通；

f）与其它评价人员交流、沟通；

g）完成审核组长交付的其它工作等。

9.3.3.3 现场审核流程

9.3.3.3.1 流程

现场审核工作流程，参看附录C。

9.3.3.3.2 说明

现场审核工作，主要应完成：

a）审查PISMSE申请者提交的文档；

b）文档审查通过后形成资格审核报告；

c）依据个人信息安全相关法规、标准和PISMSE相关标准，提出并遵守相应的PISMSE要求；

d）编制PISMSE现场审核计划；

e）设计评价指标、等级标准、评分范围和权重；

f）召开现场审核准备会议，明确PISMSE目标、职能职责、工作任务、审核计划、评价指标等；

g）进入审核现场，召开现场审核工作会议，说明现场审核计划、PISMSE要求等各项审核事项；

h）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；

i）评价人员按照分工要求，调查、分析、判断、评估PISMS运行状况；

j）判断个人信息管理者的个人信息管理情况与个人信息安全相关法规、标准及评价要求的符合性；

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结论；

m）与个人信息管理者相关人员沟通、交流；

n）验证所采取的现场审核方法的有效性；

o）审核结束，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；

r）编制并提交现场审核报告。

9.3.3.4 审核会议

9.3.3.4.1 要求

现场审核组应依据DB21/T 2702.1 9.2确立的会议规则和内容，召开相应的会议。

9.3.3.4.2 审核准备

现场审核组进入审核现场前，应召开准备会议。会议主要内容应包括：

a）明确PISMSE的目的、任务；

b）沟通，了解、熟悉个人信息管理者的基本情况、业务范围等；

c）了解资格审核报告内容及PISMS构建、实施、运行状况；

d）部署现场审核计划、审核时间、阶段和进度，以及评价员的分工范围；

e）说明评价指标设计；

f）现场审核的质量保证措施；

g）评价人员的相关专业知识培训、讲解等。

9.3.3.4.3 进入现场

现场审核组进入审核现场，应依据DB21/T 2702.1 9.2.3召开工作会议：

a）DB21/T 2702.1 9.2.3确定的主要会议内容及其它必要事项；

b）形成对个人信息管理者的初步、整体的基本认识；

c）形成对PISMS运行状况的基本了解；

d）与个人信息管理相关人员建立信任、合作的基础；

e）建立审核双方认可的信息安全承诺等。

9.3.3.4.4 审核过程

现场审核组在审核过程中，应依据DB21/T 2702.1 9.2.4适时召开工作例会：

a)）DB21/T 2702.1 9.2.4确定的主要会议内容及其它必要事项；

b）检查审核方法、样本选择；

c）检讨审核过程中可能存在的问题；

d）需要再次评估的问题；

e）需要与个人信息管理相关人员沟通、协调的问题；

f）形成一致、统一的结论。

9.3.3.4.5 审核结束

现场审核组结束现场审核后，应依据DB21/T 2702.1 9.2.5召开工作会议：

a）DB21/T 2702.1 9.2.5确定的主要会议内容及其它必要事项；

b）现场审核意见定性、定量描述、说明；

c）听取个人信息管理者相关人员的解释和说明；

d）与个人信息管理者达成共识。

9.3.3.5 调查方法

9.3.3.5.1 要求

现场审核组在审核过程中，应依据DB21/T 2702.1 9.3展开现场调查：

a）应通过现场调查获取真实的PISMSE原始数据；

b）应比较现场获取数据与社保数据的符合性、一致性和有效性；

d）应通过文档检查确认申报文档的完整性、真实性；

e）应充分了解个人信息管理者，根据实际、申报文档等设计面谈大纲和内容；

e）面谈可在审核过程中的任一阶段，根据调查需要实施。

9.3.3.5.2 面谈样本

面谈样本的选择：

a）集体面谈，样本选择应包括：

1）主管最高领导者；

2）PISMS所有相关责任主体；

3）也可根据需要选择关键部门责任主体；

b）个人面谈，样本选择应包括：

1）最高管理者（可根据实际情况选择）；

2）PISMS相关责任主体；

3）关键部门员工；

4）可根据实际需要随机选择其它员工。

9.3.3.5.3 抽查样本

可在文档检查后实施现场调查。应依据DB21/T 2702.1 9.3.3，选择适当的调查样本。应基于以下考虑：

a）了解个人信息管理者的基本情况；

b）PISMSE资格审核；

c）面谈、文档审查等。

依据DB21/T 2702.1 9.3.3.2确定的规则和其它可能的情况，选择抽查样本。

9.3.3.5.4 抽查范围

应依据DB21/T 2702.1 9.3.3.3确定抽查范围，主要应包括：

a）时间范围：PISMS构建、实施和运行的时间节点；

b）样本选择范围：根据DB21/T 2702.1 9.3.3.2确定样本覆盖的范围；

c）样本检查范围：根据样本选择范围确定样本检查节点等。

抽查范围应根据个人信息管理者个人信息管理的实际调整。

9.3.3.5.5 抽查数量

应依据DB21/T 2702.1 9.3.3.4确定的规则确定抽查数量，主要包括：：

a）总体特征：个人信息管理者内部个人信息的分布、业务特征、管理特征及各种关联关系等；

b）准确率：保证各个抽查样本覆盖个人信息管理的总体特征，不应单纯追求数量；

c）层次化：可在抽查范围内，划分评价对象的不同层次，重点层次可适当多的选取抽查样本。

9.3.3.5.6 抽查结论

抽样调查结束后，应基于面谈、文档审查和抽查过程，依据DB21/T 2702.1 9.3.3.5形成抽样调查结论。

9.3.3.6 审核实施

9.3.3.6.1 要求

DB21/T 2702.1 9.3.4.1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。

9.3.3.6.2 审核质量

9.3.3.6.2.1 调查偏差

依据DB21/T 2702.1 9.4.3，偏差类型包括：

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。

9.3.3.6.2.2 调查控制

a）应依据DB21/T 2702.1 9.4.2.2采取相应的控制措施；

b）应依据DB21/T 2702.1 9.4.2.3及时处理各种可能的问题；

c）应注意审核人员个人素养养成，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）应依据DB21/T 2702.1 9.4.4，与PISMS相关人员沟通交流，与审核组内成员互动交流。

9.3.3.7 审核结论

9.3.3.7.1 要求

应依据DB21/T 2702.1 9.5形成审核结论：

a）应累积、整理、分析现场审核过程中的所有信息；

b）应根据分析结果和资格审核报告判断、评估PISMS；

c）根据DB21/T 2702.1 9.5.2确立的问题分类原则和PISMS评估结果，明确说明存在的问题和解决建议；

d）形成公正的审核意见。

9.3.3.7.2 审核意见

应依据DB21/T 2702.1 9.5.3形成审核意见：

a）应依据7.2.2确定评分等级和评分范围；

b）应依据7.2.2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 2702.1 9.5.3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 2702.1 9.5.3 a）1）的条件，应通过PISMSE；

e）形成现场审核意见。

9.3.3.7.3 整改

现场审核等级确定为1级、2级，应依据DB21/T 2702.1 9.6整改，并提交整改报告。

现场审核组应评估整改报告：

a）如已满足DB21/T 2702.1 9.5.3 a）1）的条件，应通过PISMSE；

b）应根据DB21/T 2702.1 9.5.3 a）3）确立的原则，再次现场审核；

c）根据DB21/T 2702.1 9.5.3 b）1）确立的原则，如仍不能达到DB21/T 2702.1 9.5.3 a）1）的条件，不应通过现场审核。

9.3.3.8 现场审核报告

现场审核结束后，应依据DB21/T 2702.1 9.7形成现场审核报告。

9.4 审批和公示

9.4.1 审核

评价机构应依据DB21/T 2702.1 10.1审核现场审核组提交的PISMSE相关文档。

9.4.2 评价报告

评价机构审核通过后，现场审核组应依据DB21/T 2702.1 10.2编制PISMSE报告。

9.4.3 审批和公示

管理机构应依据DB21/T 2702.1 10.3审批评价报告。

评价机构应在审批通过后，依据DB21/T 2702.1 10.4，采取适当方式公示。

9.5 仲裁服务

参见DB21/T 2702.9《信息安全 个人信息安全管理体系评价 第9部分：仲裁指南》。

10 人员管理

参见DB21/T 2702.3《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》。

11 文档管理

应依据DB21/T 2702.1 第13章的规则完善PISMSE所有相关文档的管理。

12 过程改进

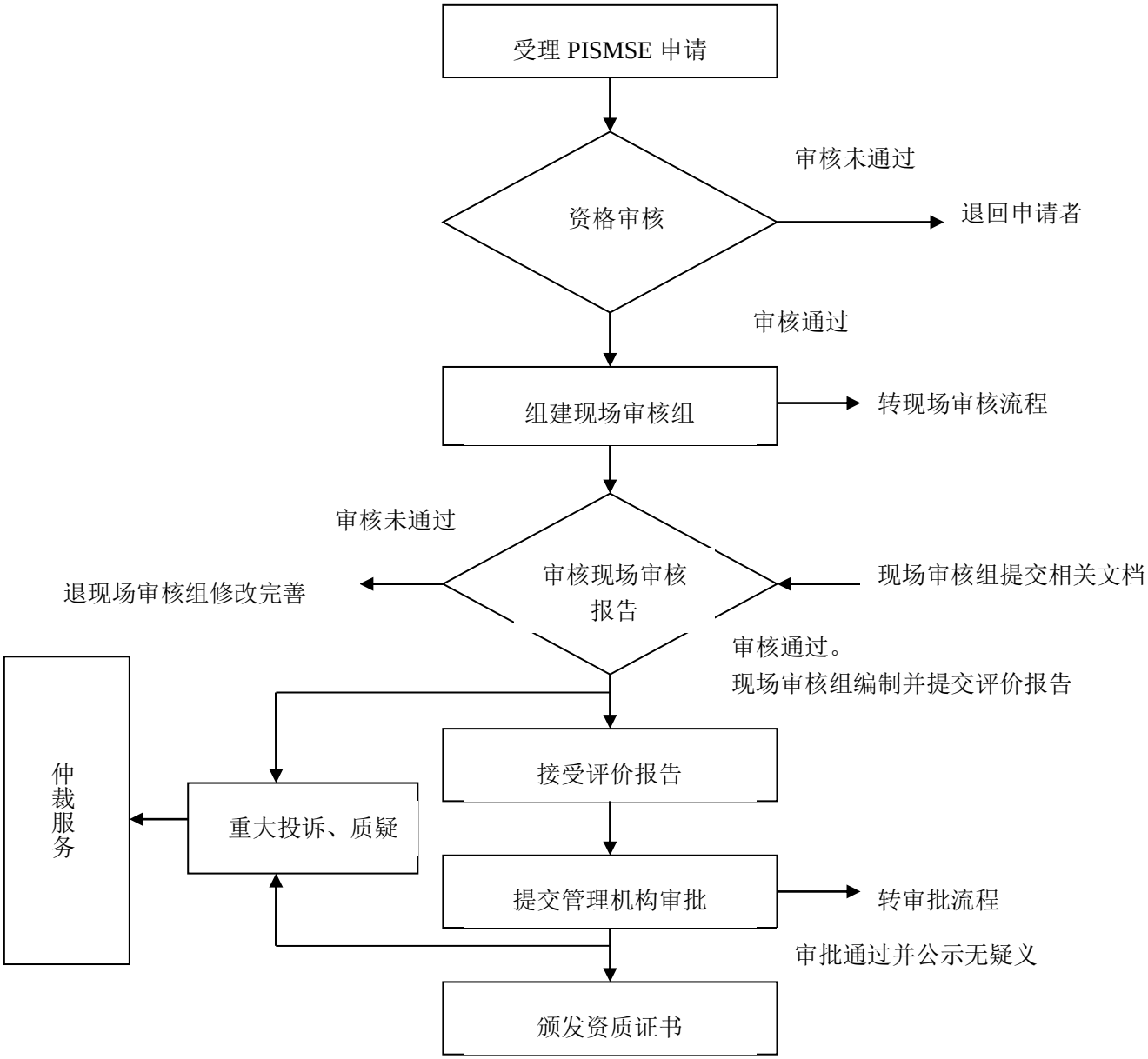
a）应依据DB21/T 2702.1 第14章确立的规则实施过程改进；

b）应参照DB21/T 1628.2 第18章和DB21/T 1628.8的过程管理方法，不断改进、完善PISMSE体系。

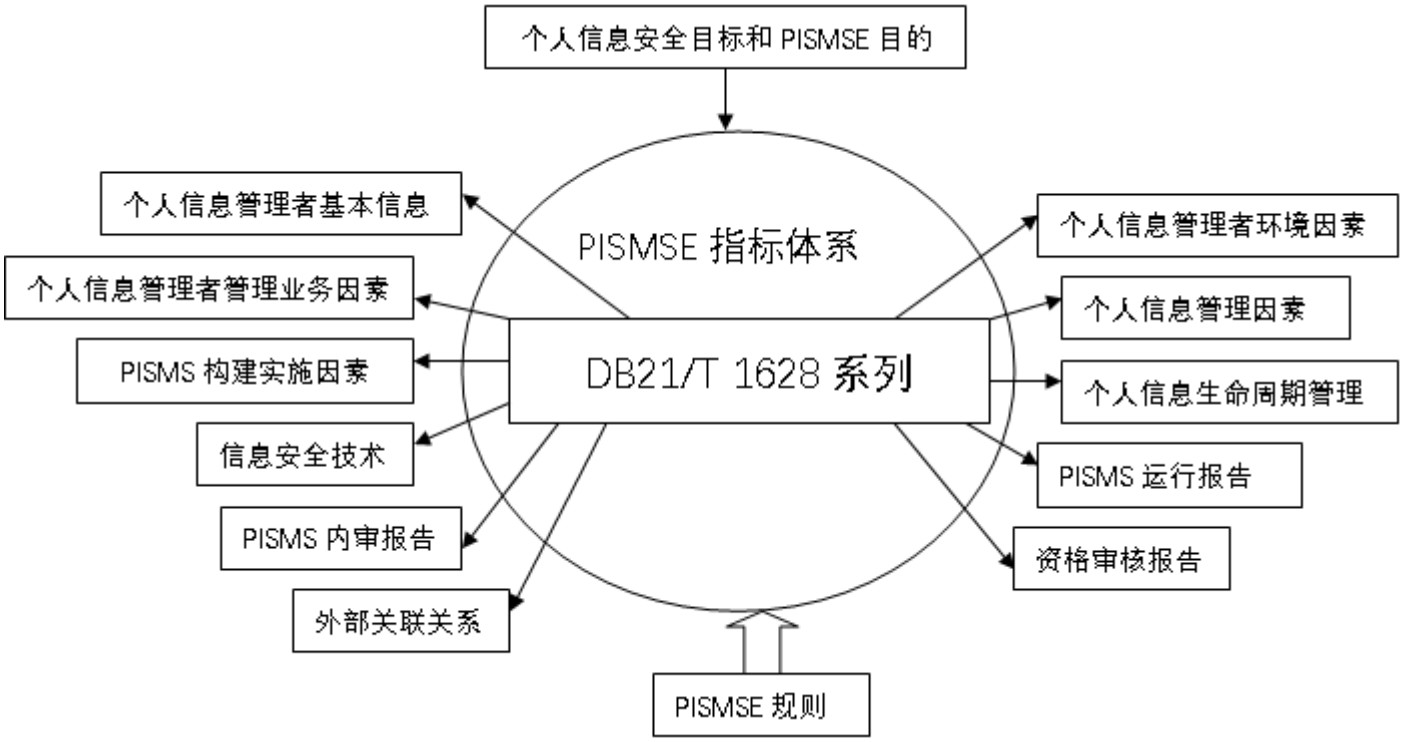
13 资格管理

参见DB21/T 2702.11《信息安全 个人信息安全管理体系评价 第11部分：资格管理》。

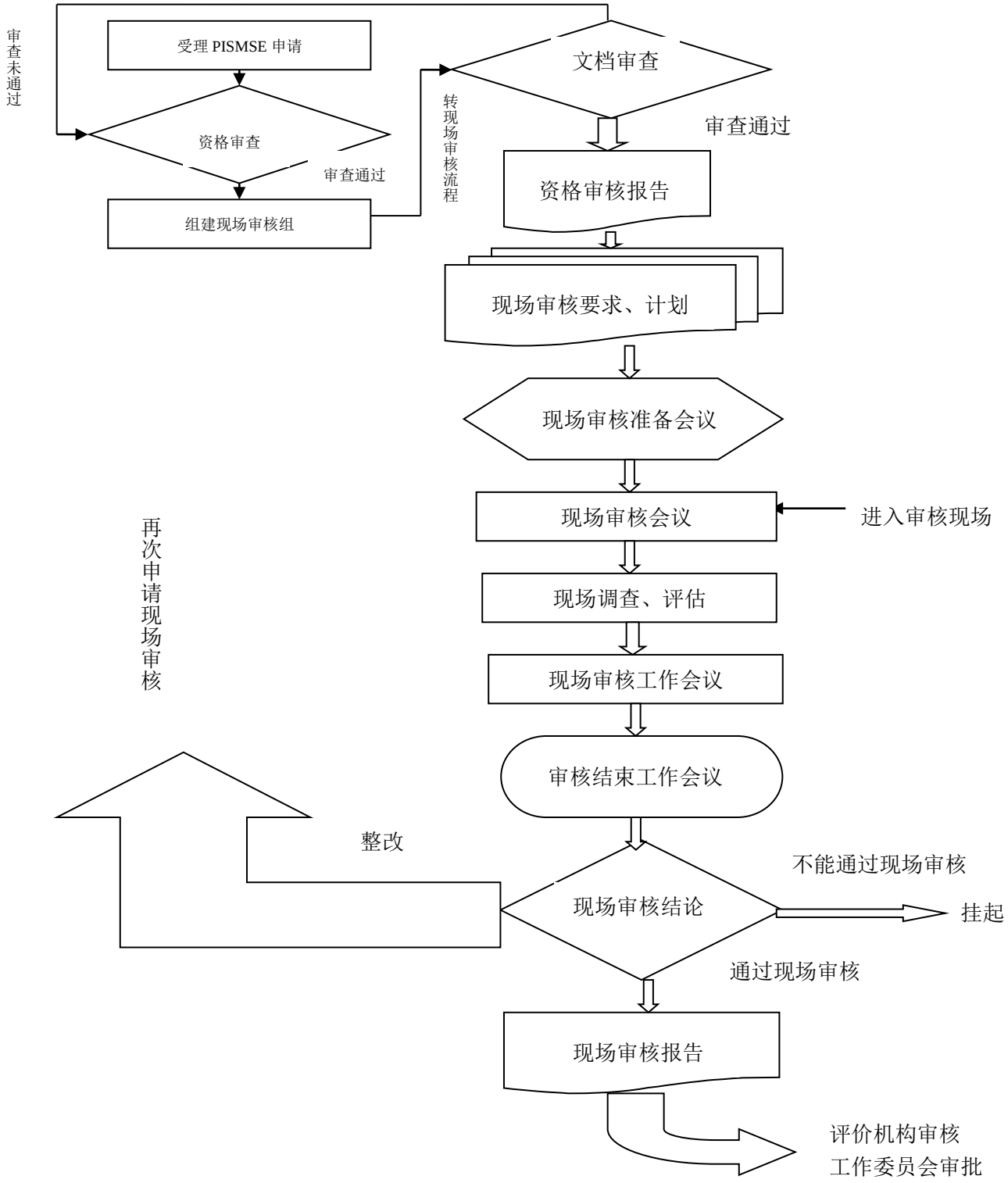
附 录 A
（规范性附录）
评价机构工作流程



附 录 B
（规范性附录）
PISMSE 指标体系结构



附 录 C
（规范性附录）
现场审核工作流程



附 录 D
（资料性附录）
PISMSE 指标体系构成示例

et	ei	ec	评分
管理机构（权重 %）	最高管理者	认知	
		支持力	
		现场调查	
	机构设置	完善	
		职责	
		效能	
		现场调查	
风险管理（DB21/T 1628.5）（权重 %）	风险源识别	风险源识别边界	
		风险源识别覆盖	
		资源风险识别	
		体系风险识别	
		现场调查	
	风险分析和处理	风险评估有效、充分	
		风险定性描述和定量分析	
		风险应对和处理措施	
		风险控制措施	
		现场调查	
管理机制（权重 %）	管理制度	规章完善、适用、合理	
		规章普及	
		规章实施情况	
		现场调查	
	宣传	宣传方法和策略	
		宣传覆盖	
		宣传内容针对性、合理性	
		效果	
		现场调查	
	培训教育	培训计划、周期	
		培训普及人群	
		培训内容针对、适用	
		培训记录完整、清晰	
		效果	
		现场调查	
	文档管理	记录完整、清晰、易读	
		文档管理方法、措施	

		文档管理安全性	
		文档备案、借阅	
		现场调查	

et	ei	ec	评分
个人信息主体权利（权重　%）	管理活动	涉及个人信息的各种活动、行为、文档的权利保障	
		涉及个人信息主体的各种活动、行为的权利保障	
		现场调查	
	业务活动	涉及个人信息业务的权利保障方式、策略	
		现场调查	
个人信息管理者（权重　%）	责任和义务	管理活动中的责任和业务	
		业务活动中履行责任、义务的方式	
		现场调查	
	能力和规则	符合 6.1 规定的规则	
		具有管理职能和服务能力	
		现场调查	
管理活动（权重　%）	原则	基本原则的解释	
	方针	与实际管理业务需求一致	
		内容清晰、明确、易读、无遗漏	
		公开发布、显见	
		改进情况	
		现场调查	
	边界	管理覆盖边界、范围清晰	
	计划	明确、清晰	
		内容详实、计划周密	
		有计划执行评估措施	
		现场调查	
	体系建设	设计明确、功能完善	
		流程清晰、有效	
		体系与业务、与其它体系融合	
		现场调查	
个人信息数据库（DB21/T 1628.3）（权重　%）	识别	个人信息分布	
		个人信息存储、保存形式	
		个人信息相关记录	
		个人信息识别率	
		现场调查	
	环境	自动处理环境的标准符合性	
		非自动处理的保存环境	

		环境的安全性	
		移动环境的安全性	
		现场调查	

et	ei	ec	评分
个人信息数据库（DB21/T 1628.3）（权重　%）	管理机制	专人负责	
		职责	
		规章制度	
		现场调查	
	管理策略	时限管理	
		状态管理	
		后处理形式	
		记录和相关文档管理	
		备案管理	
		管理控制	
		现场调查	
	事务管理	业务流程中的相关事务	
		行政管理中的相关事务	
		事务的适宜性和符合性	
		现场调查	
	风险管理	风险识别和评估（8.1）	
		应对和处理策略	
		监控和跟踪	
		应急处理机制	
		现场调查	
	二次开发	目的、权利、责任	
		方式方法	
		安全保障	
		现场调查	
获取过程	…	…	
	⋮		

附 录 E
（资料性附录）
资格审核报告示例

个人信息安全管理体系评价

Personal information security management system evaluation

资格审核报告

Qualification audit report

个人信息安全管理体系评价机构办公室

说　　明

1　本报告依据 DB21/T 1628 系列、DB21/T 2702　系列标准编制。

2　本报告由 PISMSE 现场审核组根据资格审查、文档审查结论编制。

3　本报告为实施 PISMSE 现场审核的基础。

申请受理基本信息				
申请者				
申请日期				
受理日期				
受理人		受理号		
资格审核日期		审核人		
申 请 次 数	□ 初次申请 □二次申请 □第 __ 次申请			
资格审核次数	1 2			
	通过审核最近日期：			
报告编制人		日 期		
报告审核人		日 期		

资格审查

<table>
<tr><td colspan="6">PISMSE 申请者基本信息</td></tr>
<tr><td>申请者</td><td colspan="5"></td></tr>
<tr><td>所在地址</td><td colspan="5"></td></tr>
<tr><td>生存期</td><td colspan="2"></td><td>员工人数</td><td colspan="2">人</td></tr>
<tr><td rowspan="3">说明</td><td rowspan="2">基本情况</td><td>业务范围</td><td colspan="3"></td></tr>
<tr><td>其它</td><td colspan="3"></td></tr>
<tr><td colspan="2">经营状况</td><td></td><td>资信状况</td><td colspan="2"></td></tr>
<tr><td rowspan="3">个人信息</td><td>管理</td><td colspan="4"></td></tr>
<tr><td>业务</td><td colspan="4"></td></tr>
<tr><td>其它</td><td colspan="4"></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>联系方式</td><td colspan="2"></td></tr>
</table>

PISMSE 申请资格初步审查		
审查内容	审查结果	问题说明
基本信息		
提交文档		
个人信息说明		
PISMS 说明		
个人信息安全事故说明		
PISMS 内审和运行报告		
内审整改报告		
其它需说明的问题		

资格审查结论

文档审查

PISMSE 申请提交文档审查		
审查内容	审查结果	问题说明
提交文档		
PISMS 运行状况		
计划方针等管理措施		
组织机构		
职能职责		
规章制度		
培训教育		
个人数据库管理		
风险分析		
内审		
过程改进		
其它		

需现场审核确认问题说明

整改情况说明	
审核问题	整改措施

文档审查结论

审核问题反馈说明		
审核问题	意见和建议	处理措施

资格审核意见
1.资格审查： 2.文档审查 3.整改情况：
审核意见： 报告人（签字）： 年　　月　日

附

整改报告

附 录 F
（资料性附录）
审核计划示例

个人信息安全管理体系评价

Personal information security management system evaluation

现场审核计划

Field audio plan

受 理 号：_____

申请单位：_____

制定日期：_____

评价机构：_____

个人信息安全管理体系评价机构制表

<table>
<tr><td colspan="3">审核申请者</td><td colspan="4"></td></tr>
<tr><td colspan="3">现场审核时间</td><td></td><td>审核地点</td><td colspan="2"></td></tr>
<tr><td rowspan="2">申请者基本信息</td><td colspan="6"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td colspan="3"></td></tr>
<tr><td rowspan="3">资格审核说明</td><td>一般情况说明</td><td colspan="6"></td></tr>
<tr><td>现场确认问题</td><td colspan="6"></td></tr>
<tr><td>评价依据</td><td colspan="6">DB21/T 1628 系列个人信息安全标准体系
DB21/T 2702 系列个人信息安全管理体系评价标准体系</td></tr>
<tr><td rowspan="7">现场审核组</td><td rowspan="4">成员</td><td>姓名</td><td></td><td>职务</td><td colspan="2"></td></tr>
<tr><td>姓名</td><td></td><td>职务</td><td colspan="2"></td></tr>
<tr><td>姓名</td><td></td><td>职务</td><td colspan="2"></td></tr>
<tr><td>姓名</td><td></td><td>职务</td><td colspan="2"></td></tr>
<tr><td>职责</td><td colspan="5">遵循 DB21/T 2702.1 和 DB21/T 2702.2 的规定：
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PISMS构建、实施、运行状况，理解个人信息管理者实际；
d）基于PISMS整体状况，判断、评估分工范围内的PISMS构成要素；
e）与分工范围内的个人信息管理者的相关人员交流、沟通；
f）与其它评价人员交流、沟通；
g）完成审核组长交付的其它工作等。</td></tr>
<tr><td rowspan="4">分工</td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
</table>

审核范围和重点		
评价指标说明	指标项	
	权重	
审核方法		
审核有效性		
审核安全性		
文档管理		
审核结论		
说明		

计划编制者：

附 录 G
（资料性附录）
现场审核报告示例

受理编号：

个人信息安全管理体系评价

Personal information security management system evaluation

现场审核报告

Field audit report

个人信息安全管理体系评价机构办公室

说　　明

1　本报告依据 DB21/T 1628 系列、DB21/T 2702　系列标准编制。

2　本报告由 PISMSE 现场审核组实施现场审核后编制。

版本号	制定/修改日期	事由	编制人
1.0			
1.1			
1.2			

现场审核基本信息			
申请受理日期		资格审核日期	
送审材料版本		最终材料版本	
现场审核次数	■ 初次审核 ❒ 再次审核		
现场审核时间			
现场审核地点			
资格审核人		日 期	
报告编制人		日 期	
报告审核人		日 期	
报告批准人		日 期	

需现场审核确认问题说明

基本信息			
申请者			
注 册 地 址			
现 地 址			
注 册 资 本	RMB 万元整	法人代表	
成 立 日 期		员工人数	
其它需说明的问题			

现场审核组基本信息			
组长		职务	
成员		职务	

审核报告

1 现场审核基本情况说明

2 个人信息管理者基本情况、与个人信息管理相关情况说明

3 PISMS 情况说明

4 现场审核计划（见附表）

5 现场审核方式：（抽样、抽查、面谈等）

6 现场审核内容：（根据资格审核、实际情况确定重点）

7 现场审核综述

问题说明
整改说明

现场审核意见
评价机构意见
PISMS 机构办公室 _____年___月___日

附

资格审核报告

现场审核计划

现场审核文档

整改意见书

整改报告

附 录 H
（资料性附录）
评价报告示例

受理编号：

个人信息安全管理体系评价

Personal information security management system evaluation

评价报告

Evaluation report

个人信息安全管理体系评价机构办公室

说　　明

1　本报告依据 DB21/T 1628 系列、DB21/T 2702　系列标准编制。

2　PISMS 现场审核组根据《资格审查报告》、《现场审核报告》和《公示情况说明》，形成本报告。

3　本报告将提交 PISMSE 管理机构审议。

<table>
<tr><td colspan="6">PISMSE 申请者基本信息</td></tr>
<tr><td>申请者</td><td colspan="5"></td></tr>
<tr><td>所在地址</td><td colspan="5"></td></tr>
<tr><td>成立时间</td><td colspan="2"></td><td>员工人数</td><td colspan="2">人</td></tr>
<tr><td rowspan="3">说明</td><td rowspan="2">基本情况</td><td>业务范围</td><td colspan="3"></td></tr>
<tr><td>其它</td><td colspan="3"></td></tr>
<tr><td colspan="2">经营状况</td><td></td><td>资信状况</td><td colspan="2"></td></tr>
<tr><td rowspan="3">个人信息</td><td>管理</td><td colspan="4"></td></tr>
<tr><td>业务</td><td colspan="4"></td></tr>
<tr><td>其它</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="4">现场审核组基本信息</td></tr>
<tr><td>组长</td><td></td><td>职务</td><td></td></tr>
<tr><td rowspan="3">成员</td><td></td><td rowspan="3">职务</td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

报告编制人：

日　　期：

<table>
<tr><td colspan="5">资格审核</td></tr>
<tr><td>申请受理日期</td><td colspan="2"></td><td>资格初审日</td><td></td></tr>
<tr><td>资格再审日期</td><td colspan="4">1　　2
3　　4</td></tr>
<tr><td>申请通过日期</td><td colspan="4"></td></tr>
<tr><td colspan="5">资格审查</td></tr>
<tr><td>审查日期</td><td colspan="2"></td><td>审查人</td><td></td></tr>
<tr><td>审查次数</td><td colspan="4"></td></tr>
<tr><td>问题说明</td><td colspan="4"></td></tr>
<tr><td>整改意见</td><td colspan="4"></td></tr>
<tr><td rowspan="2">整改报告</td><td>提交时间</td><td colspan="3"></td></tr>
<tr><td>整改措施</td><td colspan="3"></td></tr>
<tr><td>资格审查结论</td><td colspan="4"></td></tr>
</table>

文档审查			
审查日期		审查人	
审查次数			
问题说明			

<table>
<tr><td>整改意见</td><td colspan="2"></td></tr>
<tr><td rowspan="2">整改报告</td><td>提交时间</td><td></td></tr>
<tr><td>措施</td><td></td></tr>
<tr><td>现场确认问题</td><td colspan="2"></td></tr>
<tr><td>文档审查结论</td><td colspan="2"></td></tr>
<tr><td colspan="3">资格审核结论</td></tr>
<tr><td colspan="3"></td></tr>
</table>

<table>
<tr><td colspan="5">现场审核</td></tr>
<tr><td>现场审核时间</td><td colspan="4"></td></tr>
<tr><td>二次现场时间</td><td colspan="4"></td></tr>
<tr><td>评价指标评分说明</td><td colspan="4"></td></tr>
<tr><td rowspan="2">现场审核结论</td><td>评价总分</td><td></td><td>评价等级</td><td></td></tr>
<tr><td>审核意见</td><td colspan="3"></td></tr>
<tr><td>问题说明</td><td colspan="4"></td></tr>
<tr><td>整改意见</td><td colspan="4"></td></tr>
</table>

整改报告	提交时间	
	整改措施	
	整改效果	
整改后意见		

评价机构审核	
审核报告提交时间	
审核时间	
审核意见	
整改意见	
复审意见	

评价综述
PISMS 运行质量的考量 评价过程改进的考虑 具有一般性指导意义的问题等

附件 A：《资格审核报告》

附件 B：《现场审核计划》

附件 C：《现场审核报告》

附件 D：《整改意见书》

附件E：《整改报告》