ICS 35.020
L70

DB21

辽 宁 省 地 方 标 准

DB 21/T 1628.7—2018

信息安全 个人信息安全管理体系 第7部分：内审实施指南

Information security-Personal information security management system-Part7: Internal audit implementation 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 1628 分为 8 部分：

——信息安全 个人信息保护规范（信息安全 个人信息安全管理体系 第 1 部分：通用要求）

——信息安全 个人信息安全管理体系 第 2 部分：实施指南

——信息安全 个人信息安全管理体系 第 3 部分：个人信息数据库管理指南

——信息安全 个人信息安全管理体系 第 4 部分：个人信息管理文档管理指南

——信息安全 个人信息安全管理体系 第 5 部分：个人信息安全风险管理指南

——信息安全 个人信息安全管理体系 第 6 部分：安全技术实施指南

——信息安全 个人信息安全管理体系 第 7 部分：内审实施指南

——信息安全 个人信息安全管理体系 第 8 部分：过程管理指南等。

本部分是 DB21/T 1628 的第 7 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、孙毅、王小庚。

信息安全 个人信息安全管理体系 第7部分：内审实施指南

1 范围

本标准规定了个人信息安全管理体系内审原则、管理、管理机制和实施的基本规则和要求。

本标准适用于自动或非自动处理全部或部分个人信息的机关、企业、事业、社会团体等组织及个人。

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、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标准。

3.1.1

PISMS 内审 PISMS internal audit

PISMS内部审计。运用系统、规范的方法，监督、检查、评价PISMS构建、实施、运行的充分性、有效性、安全性和适宜性，促进PISMS的改进、完善，保障个人信息主体的权益。

3.2 缩略语

内审 internal audit

PISMS内审。

4 要求

本指南遵循DB21/T 1628.1确立的个人信息管理原则和要求，亦遵循DB21/T 1628.2确立的实施细则，重点描述和指导PISMS内部审计的约束规则。

PISMS内部审计，应同时使用DB21/T 1628.1、DB21/T 1628.2和本指南，并参照DB21/T 1628系列其它标准。

5 原则

5.1 客观性

应客观反映 PISMS 状态，保证内审真实、有效。

5.2 目的性

应明确个人信息管理者的发展目标，确立 PISMS 的实施目的。

5.3 职责性

应明确内审的管理职能、人员责任和内审机制的功能，保证内审质量。

5.4 价值性

应充分考虑个人信息管理者的管理、业务流程价值，提供充分、适宜的内审服务。

6 管理

6.1 目的

个人信息管理者应系统、科学、规范地自我评价个人信息管理的充分性、控制有效性、信息真实性和PISMS的效率和效果。

6.2 组织机构

6.2.1 最高管理者

最高管理者应是推进PISMS内审，持续改进PISMS的决策者。其责任应包括：

a）确立个人信息安全、保证管理和业务稳定运行的目标和方向；

b）明确PISMS内审的重要性，并给予所需资源等各个方面的完全支持；

c）遵循DB21/T 1628.1 7.5.2.3，选择有能力的内审代表，组建内审机构，并赋予相应权限，确保内审实施；

d）对内审过程中可能出现的各种不利因素提供决策支持；

e）内审实施过程中的内部协调；

f）批准内审职责和内审计划，并协调个人信息管理机构，组织实施内审；

g）审核、批准内审报告。如果存在实质性问题，责成个人信息管理机构整改。

6.2.2 内审代表

内审代表应是由最高管理者选聘的责任主体，依据DB21/T 1628.1 7.5.2.3，其职责应包括：

a）独立提出和制定PISMS内审计划，并报最高管理者和个人信息管理者代表；

b）代表最高管理者组建内审机构并负责日常工作；

c）明确内审人员的职责和工作边界；

d）确定内审所需资源；

e）负责内审实施和实施过程中的组织、管理；

f）协调个人信息管理机构的工作；

g）实施内审过程改进。

6.2.3 机构职责

内审机构应遵循DB21/T 1628.1 7.5.2.3和DB21/T 1628.2 10.5.1.4确立的职责：

a）明确PISMS内审的目的，编制内审制度和内审计划；

b）内审体系应独立运行、与个人信息管理机构并行；

b）内审机构应公平、公正地开展工作，不应受到干扰；

c）内审职责应明确、清晰，并切实履行；

d）跟踪、评估PISMS构建、实施过程的合理性、充分性和完整性；

e）评价管理人员、工作人员的意识、行为、活动；

f）评估PISMS运行的效率和效果；

g）跟踪、监控、评估PISMS，及时发现缺陷，提出适宜的改进、完善建议，督促PISMS改进、完善。

6.3 计划

6.3.1 要求

根据DB21/T 1628.1 12.1.2，PISMS内审代表应根据个人信息安全目标、相关法规和标准、个人信息管理者的实际制定内审计划，确定适当时间，监控、检查PISMS实施、运行的有效性、充分性和适宜性，并报最高管理者。

6.3.2 目标

内审应确定 PISMS 的目标、个人信息管理措施、PISMS 实施过程是否达到：

a）符合个人信息安全相关法规、规范要求；

b）个人信息安全目标、措施和过程符合个人信息安全需求；

c）个人信息安全风险得到有效、充分的识别、控制；

d）个人信息管理适宜、安全、有效；

e）PISMS 设计、构建充分、适宜、有效；

f）PISMS 实施、运行有效；

g）过程改进有效实施等。

6.3.3 对象

PISMS 内审的对象，应是个人信息生命周期内个人信息管理的所有活动、行为及相关因素。主要应包括：

a）最高管理者；

b）个人信息管理者涉及个人信息及与此相关的部门及其责任人；

c）个人信息管理责任主体相关责任人；

d）PISMS 构建、实施、运行；

e）个人信息管理者收集、处理、使用、利用个人信息的行为；

f）员工意识和行为等。

6.3.4 责任者

PISMS 内审代表可以指定必要、适宜的内审责任人：

a）PISMS 内审机构相关人员；

b）各相关部门内审责任人；

c）其他适宜的相关人员。

6.3.5 策略和方法

内审管理策略和方法，主要应包括：

a）内审代表应适当介入个人信息管理者代表的工作，并提出合理地意见和建议；

b）内审机构应全程参与个人信息管理工作，监督PISMS的构建、实施和运行；

c）内审可在PISMS构建、实施、运行过程中根据实际情况分阶段实施；

d）内审可参照DB21/T 2702.1确定的原则和方法实施；

e）应适时评估内审风险、风险影响和结果，明确风险管理措施。

6.3.6 周期

内审代表应在 PISMS 构建、实施、运行后，根据个人信息安全目标、PISMS 评价要求和规则、内审计划，确定适当周期和时间，监控、检查、审计 PISMS：

a）PISMS 构建、实施过程中的阶段性审计；

b）PISMS 构建、实施完成后，应运行 3 个月后实施一次审计；

c）PISMS正式运行后的审计周期不应长于一年；

d）过程改进完成后，应重新实施全体系内审。

6.4 控制

内审控制措施，主要应包括：

a）内审代表应根据内审计划，适时评估内审机制的效能和内审效果，随时检查、修正内审缺陷，并监督内审计划的实施；

b）内审代表应依据内审计划，会同个人信息管理者代表适时评估内审风险及相应的管理措施。

6.5 协调

在内审实施过程中，应注意协调个人信息管理者内部各不同部门，以及个人信息管理机构。协调活动应保证PISMS内审的协调性、充分性和有效性等。

7 管理机制

7.1 制度

遵循DB21/T 1628.1 7.5.2.3确立的职责，内审机构应制定相应的管理制度，约束内审责任人员的行为。主要宜包括：

a）管理规定；

b）职责和责任；

c）人员管理；

d）过程管理；

e）缺陷发现和改进、完善；

f）缺陷追溯和责任；

g）文档管理；

h）内审报告等。

7.2 人员管理

遵循DB21/T 1628.1 7.5.2.3确立的职责，PISMS内审责任人员应遵循个人信息安全相关法规、规范、规章，独立、公平、公正的开展PISMS内审工作。内审责任人员应具有：

a）较丰富的个人信息安全专业知识、经验；

b）PISMS全生命周期的实践经验；

c）明确内审权限、责任，避免不作为、渎职和其它未经授权的行为；

d）独立、公正的思维方式，坚持正确己见的负责任的立场；

e）更新个人信息安全知识及其它相关知识，以适应科技、管理、知识、市场、社会等的变化。

7.3 培训教育

内审人员应定期接受培训和学习，以便适应个人信息管理者，及技术、管理、应用、社会需求的变化对个人信息管理的要求。

依据7.2，内审人员的培训应与DB21/T 1628.1 8.3.2的要求有所区别。

7.4 文档管理

7.4.1 记录

在内审过程中，应依据DB21/T 1628.1 8.5，记录内审相关的所有活动和行为，并依据DB21/T 1628.2 12.6 形成个人信息管理文档。

7.4.2 备案

应依据DB21/T 1628.1 8.5，建立备案管理制度。

8 实施

8.1 内审阶段

8.1.1 PISMS 构建

在 PISMS 设计、构建过程中，内审代表应主要审计：

a）最高管理者的意识和决策；

b）个人信息管理者代表的知识、专业能力；

c）个人信息安全法规、标准的理解；

d）个人信息管理计划的合理性和有效性；

e）PISMS 设计计划的合理性、充分性和规范性；

f）个人信息安全风险评估；

g）缺陷改进等。

8.1.2 PISMS 实施

在 PISMS 实施过程中，内审代表应组建内审机构，参与实施审计。主要审计应包括：

a）个人信息安全相关法规、标准的遵从度；

b）个人信息管理机构相关责任主体的知识、专业能力；

c）个人信息管理机构相关责任主体的职责和责任；

d）PISMS 各项管理机制的合理、充分；

e）个人信息管理计划的实施；

f）个人信息管理边界的覆盖；
e）个人信息安全风险评估的充分性；
f）缺陷改进；
g）PISMS 安全性评估等。

8.1.3 PISMS 运行

依据 6.2.6，PISMS 应在构建、实施完成并运行 3 个月后实施内审，审计应主要包括：
a）最高管理者及与个人信息相关各主要管理、业务部门管理者的认知；
b）个人信息管理机构相关责任主体职责和责任的遵从度；
c）个人信息管理相关人员对个人信息安全相关法规、标准和知识的理解；
d）个人信息安全目标、管理策略、管理机制和相关行为的合法性、合规性：
1）管理策略应参看 DB21/T 1628.1 7；
2）管理机制应参看 DB21/T 1628.1 8；
3）相关行为应遵从 DB21/T 1628.1 6 的规则；
e）个人信息管理相关责任主体的效能；
f）个人信息安全风险管理的理解和风险评估的充分性、有效性；
g）个人信息生命周期内的安全性评估；
h）个人信息安全宣传、教育的效果；
i）PISMS 所需各种类资源配置和安全状况；
j）个人信息安全管理技术和相应机制的可靠性和有效性；
k）个人信息管理机构与个人信息管理者内、外部的协调、合作；
l）个人信息管理与业务、PISMS 与其它管理体系的融合度；
m）违规、缺陷处理；
n）PISMS 效能和安全性评估；
o）改进、完善意见和建议等。

8.1.4 过程改进

内审的过程改进阶段，应参照 DB21/T 1628.2 18 实施。

8.2 要求

内审实施应考虑：
a）内审应由个人信息管理者代表和 PISMS 内审代表共同组织实施；
b）内审应遵从 DB21/T 1628 系列各个标准和 DB21/T 2702.1 确立的规则；
c）遵循 DB21/T 1628.1 12.1 的规则，PISMS 内审代表应根据相关法律、规范和实际需求制订 PISMS 内审计划；
d）PISMS 正式运行后，应根据 6.2.6 确定适宜的内审周期，根据个人信息管理者的运营状况，管理、业务、人员、环境变化，风险跟踪变化，体系运行状况等，适时实施内审；
e）最高管理者、各主要管理、业务部门管理者、个人信息管理者代表不应影响 PISMS 内审代表的独立性；
f）内审结束后，内审代表应根据内审计划评估内审质量，并制定改进、完善计划。

8.3 报告

PISMS 内审实施后，应形成 PISMS 内审报告。报告应包括：

a）内审目标和范围；
b）内审内容；
c）PISMS 实施、运行状况；
d）各部门、各分支机构的个人信息管理状况；
e）问题说明及评判依据；
f）整改建议；
g）内审风险、内审质量说明等。
PISMS 内审报告，应报最高管理者和个人信息管理者代表。

8.4 例外

PISMS 内审的例外情况，应包括：
a）PISMS 内审代表所在部门的内审应指定其他 PISMS 内审责任人实施；
b）PISMS 内审责任人均不应审查其所在部门的个人信息管理状况；
c）如在 3 个月内出现严重的个人信息安全事故，应参照相关标准处理。