ICS 35.020
L70

DB21

辽　宁　省　地　方　标　准

DB 21／ T1628. 5—2014

信息安全　第 5 部分:个人信息安全风险管理指南

Information Security-Part5：Personal information security risk management guidelines

2014－07－15 发布　　2014－09－15 实施

辽宁省质量技术监督局　　发 布

目 次

前　言

DB21/T1628 分为 7 部分：

——信息安全 第 1 部分：个人信息保护规范

——信息安全 第 2 部分：个人信息安全管理体系实施指南

——信息安全 第 3 部分：个人信息数据库管理指南

——信息安全 第 4 部分：个人信息管理文档管理指南

——信息安全 第 5 部分：个人信息安全风险管理指南

——信息安全 第 6 部分：个人信息安全管理体系安全技术实施指南

——信息安全 第 7 部分：个人信息安全管理体系内审实施指南。

本标准是 DB21/T1628 的第 5 部分。

本标准依据 GB/T1.1—2009《标准化工作导则　第 1 部分：标准的结构与编写》制定。

本标准由大连市经济和信息化委员会提出。

本标准由辽宁省经济和信息化委员会归口。

本标准主要起草单位：大连软件行业协会、大连交通大学。

本标准主要起草人：郎庆斌、孙鹏、张剑平、尹宏、杨万清、曹剑、王开红。

引　言

0.1　综述

风险是“不确定性对目标的影响”。即 “风险是由于从事某项特定活动过程中存在的不确定性而产生的经济或财务的损失、自然破坏或损伤的可能性” （美国 Cooper D．F 和 Chapman C．B《大项目风险分析》）。

由于个人信息处于复杂、多变的环境中，呈现出多样性，因而，个人信息安全风险发生的可能性，随环境的变化、个人信息多样态的变化，风险因素亦随之增加或减少，风险事件发生的可能性亦随之增大或减小，可能产生不同的风险影响。

个人信息安全风险管理就是识别、分析、评估个人信息管理者运营中，各种可能危害个人信息和个人信息主体权益的风险，并在此基础上，采取适当的措施有效处置风险。是以可确定的管理成本替代不确定的风险成本，以最小的经济代价，实现最大安全保障的科学管理方法。

0.2　个人信息安全风险管理的必要性

在个人信息生命周期内，个人信息以不同的样态存在，既依存于业务亦依存于管理，具有不同的风险因素。涉及个人信息安全风险的来源是多样的，依个人信息生命周期：

a）个人信息获取过程：

1）个人信息收集风险（收集目的、收集技术、方式和手段等）；

2）个人信息间接收集风险（收集目的、来源、第三方背景、安全承诺等）；

b）个人信息处理过程：

1）个人信息使用风险（使用目的、使用方法和范围、使用背景等）；

2）个人信息提供风险（使用目的、使用方法和手段、接受者背景、安全承诺等）；

3）个人信息处理风险（处理目的、处理方式、处理方法和手段、后处理方式等）；

4）个人信息委托风险（委托目的、委托接受人、委托回收、安全承诺、回收方式等）；

5）个人信息传输风险（传输方式和手段、传输的安全措施等）；

c）基于生命周期的过程管理：

1）个人信息管理风险（个人信息管理者的素质、权利和义务、管理方式等）；

2）个人信息安全管理体系风险（体系缺陷、漏洞等）；

等等。所有个人信息收集、处理、使用等行为，也都存在个人信息正确性、完整性和最新状态的风险。识别、评估、判断个人信息的潜在价值、安全威胁，是个人信息管理的基础，也是个人信息安全管理体系构建、实施、运行的安全基础。

0.3　个人信息安全风险管理评估

评估个人信息安全风险管理，包括：

a）资源的影响：资源以多种形式存在，其所依存的管理、业务关联不同，具有不同的安全属性和价值，因而存在不同的安全风险；

b）管理脆弱性：在个人信息管理者的管理体系、机制中，行政管理、员工管理、业务持续性等多

方面存在固有的缺陷，因而存在某一特定环境、特定时间段发生风险的可能性；

c）技术脆弱性：由于资源存在缺陷或漏洞，因而，所采取的技术管理措施存在必然的风险；

d）个人信息安全管理体系的影响：个人信息安全管理体系（包括管理机制、内审机制、安全机制、过程改进、认证机制等）及标准、规范等存在设计缺陷，可能引发不同的安全风险。

0.4 风险管理基准

本指南为个人信息安全管理体系提供个人信息安全风险管理的基准和支持。但是，本指南并不提供任何特定的个人信息安全风险管理方法。个人信息管理者应根据管理及业务特点、环境因素、特定的个人信息安全管理体系及风险管理范围等，确定适合自身的风险管理方式。

依据本指南的规则，实施个人信息安全风险管理存在多种方式。

0.5 与其它标准体系的兼容性

本指南支持其它国际、国内信息安全标准、风险管理标准及相关标准的一般概念和规则，并与其协调一致，相互配合或相互整合实施和运行。

0.6 规定

本指南各条款所指“风险管理”、“风险评估”、“风险处理”、“风险应对”及其它“风险 XX”等，均指“个人信息安全风险 XX”。如“风险管理”即为“个人信息安全风险管理”等。

个人信息安全风险管理指南

1 范围

本指南为个人信息安全管理体系构建、实施、运行中实施风险管理提供指导和帮助。

本指南适用于个人信息管理者内关注个人信息安全的各级管理者和员工，及为个人信息安全管理体系构建、实施和运行提供支持的相关组织。

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 1628.1-2012《信息安全-个人信息保护规范》

DB21/T 1628.2-2013《信息安全-个人信息安全管理体系实施指南》

DB21/T 1628.4-20xx《个人信息安全-个人信息安全管理体系文档管理指南》

DB21/T 1628.6-20xx《个人信息安全管理体系安全技术实施指南》

3 术语和定义

DB21/T 1628.1 界定的以及下列术语和定义适用于本标准。

3.1

风险 risk

从事某项特定活动中存在的不确定性对活动目标的影响。

3.2

资源 resources

信息、信息系统、生产、服务、人员、信誉等有价值的资产。

3.3

个人信息安全风险 personal information security risk

个人信息收集、管理、处理、使用存在的缺陷和漏洞导致安全事件发生并产生相应影响。

注：本指南所指“风险”均为“个人信息安全风险”。

3.4

风险管理 risk management

评估各种可能危害个人信息和个人信息主体权益的风险，采取适当的措施有效处置风险。以最小的经济代价，实现最大安全保障的科学管理方法。

3.5

风险识别 risk identification

发现、记录、描述危害个人信息和个人信息主体权益的风险因素的过程。

3.6

风险评估 risk assessment

识别风险因素，分析风险因素的危害，判断风险因素导致安全事件的可能性和可能产生的影响。

3.7

风险规避 risk avoidance

采取有效的管理、技术措施，或更改风险管理计划，消除风险或风险发生的条件。

3.8

风险弱化 risk mitigation

采取有效的管理、技术措施，将风险和可能的影响降低到可以接受的水平。

3.9

风险转移 risk transfer

与其它管理体系、或与其它相关组织分担风险损失和影响。

3.10

风险接受 risk acceptance

接受可能的风险损失和影响。

3.11

残余风险 residual risk

实施风险管理，采取安全措施后，仍然可能存在的风险。

4 要求

本指南遵循 DB21/T 1628.1《信息安全 个人信息保护规范》确立的个人信息安全原则和要求，亦遵循 DB21/T 1628.2《信息安全 个人信息安全管理体系实施指南》确立的实施细则，重点描述和指导个人信息安全管理体系构建、实施、运行中个人信息安全风险的评估、处理、监控和持续的过程改进。

实施个人信息安全风险管理，应同时使用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》和本指南，并参照DB21/T 1628系列其它标准。

5 风险管理概述

5.1 风险因素

风险因素包括

a）危险因素：存在可能突发或瞬时发生个人信息危害的因素；

b）危害因素：逐渐累积形成个人信息危害的因素。

示例：危险因素的事例：

a）自然灾害；

b）载有个人信息的介质突然丢失；

c）IT 设施突然受到攻击等。

危险因素分为可以预测的和不可预知的，可预测的应有必要的预防措施；不可预测的应有应急机制。

注：危险因素和危害因素是相对的，在一定条件下可能转化。当弱化个人信息安全管理时，危害因素逐渐累积，可能转变为危险因素；如果重视个人信息安全管理，则有可能规避、弱化可能存在的危险因素，并逐步降低风险等级，直至消弭。

5.2 风险类别

根据危险或危害因素分类，便于识别和分析个人信息安全风险。按照风险发生的直接原因，个人信息安全风险宜分为 5 类：

a）业务性的：涉及个人信息的业务流程中存在的风险，如：

1）业务流程的安全模式；

2）业务团队的管理模式；

3）业务管理方式；

4）IT 基础设施的管理模式等。

b）管理性的：涉及个人信息的经营管理中存在的风险，如：

1）关键部门的管理方式；

2）个人信息的管理模式；

3）网络应用方式；

4）管理人员的职责

5）个人信息安全管理体系设计缺陷等。

c）环境性的：个人信息管理者的运营场所与个人信息安全相关的环境及个人工作位置与个人信息安全相关的环境存在的风险，如：

1）环境管理（自然状况）；

2）出入管理；

3）关键部门（核心区域）管理方式；

4）相关信息（文档等）的管理方式；

5）个人终端及周边环境的管理等。

d）行为性的：与个人信息相关个人的行为可能存在的安全风险，如：

1）管理人员行为规范；

2）业务人员的行为规范；

3）IT 基础设施管理人员的行为规范；

4）个人信息管理相关负责人的行为规范；

5）个人信息安全管理体系内审人员的行为规范；

6）其他人员应遵循的行为准则等。

e）心理性的：基于人性弱点可能产生的个人信息安全风险，如：

1）电话交谈；

2）诱使开门；

3）垃圾；

4）闲谈；

5）可能的网络聊天

6）可能的网络技术欺骗等。

注：任何类型的个人信息安全风险，均与资源管理、技术策略相关。

5.3 风险管理职责

风险管理过程应是针对个人信息管理者整体，包括各部门、物理区域、环境、业务及所有资源。

实施风险管理人员应包括最高管理者、各级管理人员、个人信息管理相关负责人及其他与个人信息相关人员。其责任如表 1 所示。

表1 个人信息管理相关人员的责任

相关人员	责任
最高管理者	1 实施风险管理的决策者 2 管理者的决心和意识
各级管理人员	1 自身的行为和意识 2 本部门风险的理解和认识 3 风险管理过程的组织和协调
个人信息管理相关负责人	1 岗位职责的履行 2 所在部门的监督和沟通 3 风险应对措施 4 跟踪和监控
其他相关人员	1 自身的行为和意识 2 岗位职责的履行

5.4 风险管理实施

5.4.1 过程

风险管理的实施过程，应包括：

a）个人信息管理者代表应制定适宜、充分、有效的风险管理计划、风险管理流程和风险管理策略；

b）确定所有相关人员的责任；

c）全体员工的培训；

d）实施风险管理过程；

e）跟踪、监控风险变化；

f）过程改进。

6 个人信息安全风险管理过程

风险管理是动态、持续的，风险管理过程是可控的。风险管理过程如图1所示。

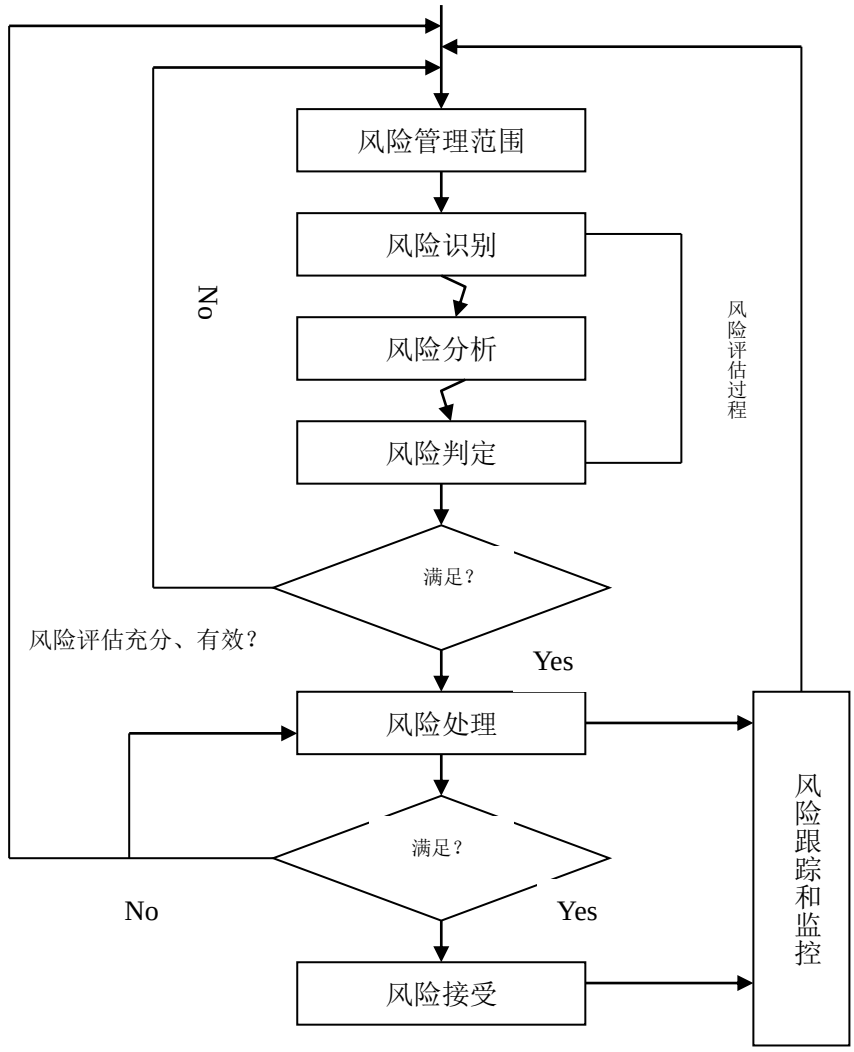

图1 风险管理过程

风险管理过程如图1：

a）确定风险管理范围：确认个人信息相关资源，资源优先级，评估损失及影响程度，以确定风险管理边界；

b）风险评估：如果风险评估充分、有效，可以采取有效的风险应对措施；否则，重新确定范围，进入新的循环；

c）如果风险应对措施合理、有效，残余风险降低到可接受水平；否则：

1）重新进行风险处理；

2）重新确定风险范围，进入新的循环；

d）风险处理、风险接受后，应持续跟踪、监控风险变化。

风险管理应采用PDCA模式，改进过程如图2 所示。

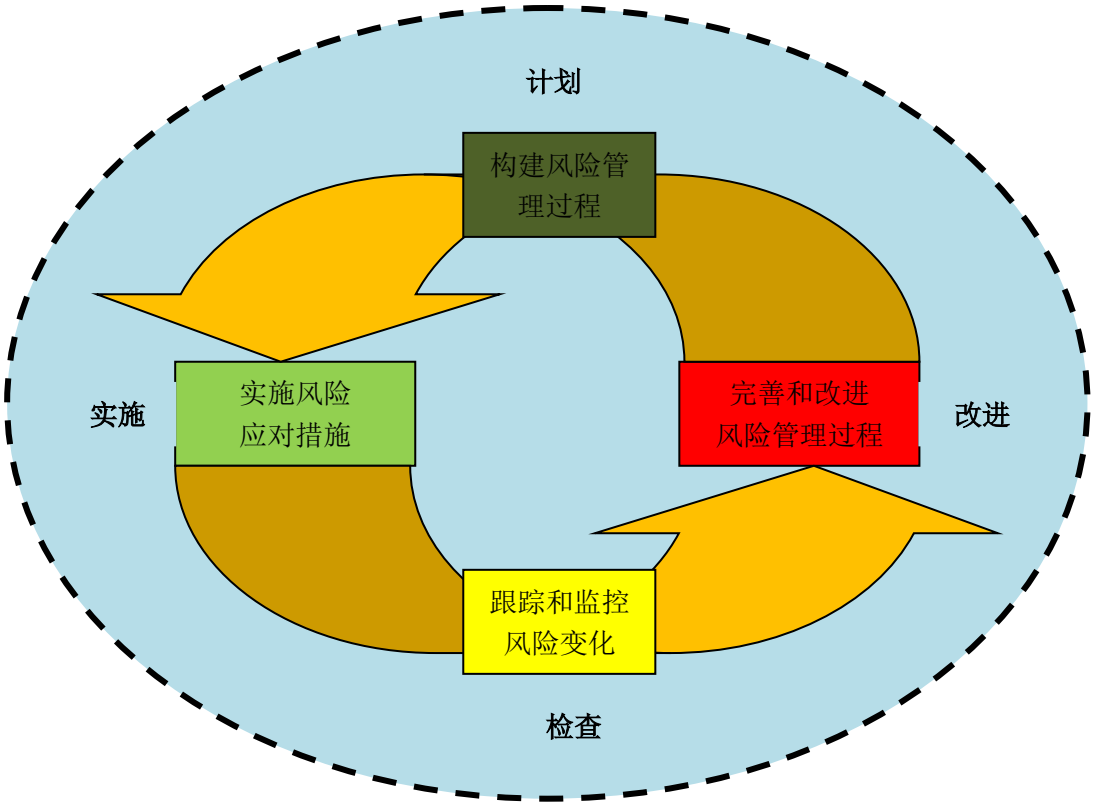

图2　适于风险管理过程的 PDCA 模式

表2描述了PDCA四个阶段的风险管理活动：

表2　PDCA 四个阶段的风险管理活动

PDCA	风险管理活动
计划	风险管理范围 风险评估 风险处理 风险接受
实施	实施风险应对措施
检查	持续跟踪、监控风险变化
改进	完善、改进风险管理过程

7　风险管理范围

7.1　资源

应识别与管理、业务涉及个人信息部分关联的各种资源。（参见 DB21/T1628.2 第 8 章）。

注：风险管理范围涵盖了个人信息管理者所有与个人信息相关的资源。

7.2 范围界定

确定风险管理的范围，应考虑：

a）个人信息管理者的运营战略、管理结构、业务模式；

b）个人信息管理机构的职能；

c）个人信息管理方针；

d）资源管理（参见 DB21/T1628.2 第 8 章）；

e）依据风险类别确定风险管理的边界；

f）影响风险管理的约束条件等。

8 风险评估

8.1 原则

风险评估是在风险管理范围内，识别与个人信息相关联的资源，识别个人信息的安全风险，分析、判断风险发生的可能性和可能的影响。

风险评估的原则，宜遵循：

a）个人信息安全相关法规、规范的要求；

b）个人信息管理者的管理、业务模式和发展战略；

c）与个人信息相关资源的重要程度；

d）风险等级；

e）与所涉及个人信息相关各方的权益。

8.2 风险识别

8.2.1 资源识别

8.2.1.1 资源风险

资源风险主要表现为：

a）资源依赖度：涉及个人信息的管理、业务对各类资源的依赖程度，依赖度越高，风险越大；

b）资源价值：与管理、业务涉及个人信息部分关联的各种资源，依赖程度越高，价值越大，风险越大；

c）资源管理者、使用者：个人责任；自然的或人为的、意外的或故意的行为等对资源的潜在风险；

d）环境因素：资源所处环境的安全。

8.2.1.2 资源风险确认

应对每一项可识别的需要保护的资源，确认：

a）关键的、需重点防护的：资源依赖度高、价值高的资源；

b）次要的但也需保护的：资源依赖度相对较高，具有较高的价值的资源；

c）暂不需专门关注的：资源依赖度相对较低，资源价值较低。

8.2.1.3 资源风险描述

在风险管理范围内，应识别、描述与管理、业务涉及个人信息部分关联的各种资源：

a）该类资源的详细信息；

b）资源与个人信息的关联度；

c）资源的责任者和职能等。

8.2.1.4 资源风险跟踪

a）资源识别是个人信息生命周期存续期间相关资源的识别。应关注资源与个人信息安全的关联，在资源识别中，应注重威胁个人信息生命周期各个环节的风险；

b）个人信息安全风险发生的可能性因环境、管理、业务及个人信息多样态等的变化动态变化，因而对资源的关注度也随之变化。跟踪、监控风险变化，亦应识别资源的重要程度。

示例：典型实例，如表 3。

表3 资源识别典型实例

资源识别	风险描述	应对措施
复印机 打印机、传真机输出资料	所涉及个人信息泄露、丢失	强化管理：如权限、责任人职能等
员工门禁卡	丢失、转借	强化管理措施、宣传和教育
身份证、护照、驾驶证等	泄露 复印件被盗取或者丢失	强化管理措施、宣传和教育
网络受到攻击	个人信息泄露	加强技术和管理措施
笔记本无线网卡上网	个人信息泄露	禁止或采取技术和管理措施

8.2.2 管理体系风险识别

个人信息安全管理体系构建、实施、运行过程中的风险识别，是体系持续改进和完善的保证。个人信息安全管理体系安全风险主要表现为：

a）最高管理者的意志和意识：如果最高管理者仅仅选择形式，则体系形同虚设。

b）个人信息管理机制的设计：管理机制设计不合理，将造成管理机构职责不清、管理制度生搬硬套、员工个人信息安全意识不清等；

c）技术管理：保障个人信息安全的信息安全技术，如网络安全、存储安全、环境安全、传输安全等，应与整体信息安全统一规划、设计，并考虑个人信息安全的特殊性；

d）业务流程管理：应充分考虑业务流程中与个人信息关联的风险因素的管理策略；

e）过程改进缺陷：应注意个人信息安全管理体系在过程改进中可能引发的潜在威胁；

8.2.3 识别约束

在风险识别中，应确定个人信息安全风险源及如何发生、以什么方式发生、发生位置、发生原因等。

8.3 风险分析

基于风险管理范围，在风险分类并识别后，定性描述分析和确认的各类风险的特征、发生的可能性、频度、显性或潜在的影响的风险等级，如表 4—表 8 示例。

表4　业务性风险等级描述

风险因素	风险等级				
	1	2	3	4	5
业务性的风险因素	不涉及个人信息	极少涉及个人信息，风险发生的可能性极小	涉及少量个人信息，存在风险但发生的可能性较小	涉及个人信息，存在较大风险且发生的可能性较大	涉及个人信息，发生个人信息安全风险的可能性很大

表5　管理性风险等级描述（1）

风险因素	风险等级				
	1	2	3	4	5
管理性的风险因素	不涉及	极少涉及个人信息，风险发生的可能性极小	涉及部分个人信息，存在风险但发生的可能性较小	涉及个人信息，存在较大风险且发生的可能性较大	发生个人信息安全风险的可能性很大

表6　管理性风险等级描述（2）

风险因素	风险等级				
	1	2	3	4	5
管理性的风险因素（技术管理）	不涉及	相应技术措施相对完善，缺陷被使用的可能性极小	相应技术措施存在一般性的缺陷，被使用的可能性较大	相应技术措施存在严重缺陷，易于被使用	未采取或仅采取少部分技术措施，风险极大

表7　环境性风险等级描述

风险因素	风险等级				
	1	2	3	4	5
环境性的危险或危害因素	无风险	在整体环境或个人工作环境中极少存在个人信息安全隐患，风险发生的可能性极小	在整体环境或个人工作环境中存在部分个人信息安全隐患，存在风险但发生的可能性较小	在整体环境或个人工作环境中存在个人信息安全隐患，存在较大风险且发生的可能性较大	在整体环境或个人工作环境中存在很大的个人信息安全隐患，极易发生风险

表8　行为性风险等级描述

等级 风险因素	1	2	3	4	5
行为性的风险因素	无行为危险	员工行为存在极少个人信息安全隐患，风险发生的可能性极小	员工行为存在发生个人信息安全隐患的可能，存在风险但发生的可能性较小	员工行为存在个人信息安全隐患，存在较大风险且发生的可能性较大	员工行为存在很大的个人信息安全隐患，极易发生风险且发生的可能性较大

注：通常采用定性描述，获得一般性的风险描述，并可发现重大安全隐患。对发现的重大安全隐患可以采用更准确或定量的分析。

8.4　风险判定

8.4.1　判定原则

风险影响判定，宜遵循以下原则：

a）违背个人信息安全相关法规、规范的情况；

b）个人信息主体权益损失程度；

c）个人信息准确性、完整性和时效性的确定；

d）资源风险的确定；

e）风险等级确定

f）经营损失的确定；

g）声誉损失。

8.4.2　风险影响

根据风险等级和风险判定原则，可判定风险可能产生的影响。影响可以分为3级，如表9所示。

表9　风险影响

风险等级	影响		
	1	2	3
	几乎无影响	不构成严重事故，但仍造成一定损失：业务受到一定影响；有一定经济和声誉损失	严重损害个人信息主体权益，影响极大：业务受到极大影响；经济和声誉有很大损失

9　风险处理

9.1　风险处理原则

应根据风险评估的结果，选择、实施适宜的风险应对措施，将风险控制在可接受的范围内。风险处理原则包括：

a）可能完全消除的风险，应完全消除；

b）不可能完全消除的风险，应尽可能采用技术和管理措施，规避、弱化或转移风险；

c）应考虑人的心理承受和行为能力；

d）应通过内审检测风险是否得到控制；

e）应通过技术、管理改进风险应对措施；

f）应制定应急计划和应急处理流程。

注：可能采用的安全技术，参见DB21/T1628.6《信息安全 个人信息安全管理体系安全技术实施指南》。

9.2 风险接受原则

9.2.1 风险接受基准

个人信息管理者应根据自身的管理和业务运行目标、特点及可接受风险能力，基于多方面情况考虑，将风险控制在可接受范围内：

a）个人信息安全相关法规、规范；

b）管理、业务模式；

c）运行模式；

d）技术管理；

e）环境因素；

f）人为因素；

g）其它因素。

9.2.2 风险接受区别

风险接受可以因下列情况不同而接受：

a）风险保持时间不同：例如，某项业务活动中风险存在时间不同，采取不同的风险应对方式，将风险降低到可接受程度；

b）各类管理者对风险的理解不同，形成风险评估差异，而采取不同的风险应对措施，但残余风险是可接受的；

c）风险是不可接受的，但承诺并确认在确定时间内将风险降低到可接受程度。

9.3 风险处理方式

一般宜采用风险规避、风险弱化、风险转移和风险接受方式处理风险：

a）风险规避：如果通过风险评估，个人信息安全风险是不可接受的，可以采用避免使用资源风险高的资源；改变运行环境；停止或取消业务、管理计划或活动（如果可能）等方式规避风险；

b）风险弱化：对高资源风险采取适宜的保护措施避免或降低风险。如 IT 基础设施的防护、个人信息数据库的防护、备份容灾、应急处理等。风险弱化应考虑：

1）注意管理、技术、环境等因素，考虑成本控制，选择适宜的措施；

2）注意安全防护措施的约束条件，如技术条件、管理成本、员工能力、环境因素等；

3）应在风险弱化后，重新实施风险评估，确定保护措施是适宜、充分、有效的。

c）风险转移：鉴于在个人信息安全管理中，风险转移的复杂性，不建议采用。

d）风险接受：通过评估，可以不采取进一步的风险处理措施，接受风险可能带来的影响。

9.4 残余风险

残余风险是采取风险处理措施后，仍然存在的风险，包括：

a）可以接受的风险；

b）风险评估中遗漏的风险，仍存在发生的可能性。

应在个人信息安全管理体系运行中跟踪、监控残余风险，随时采取相应的应对措施。

10 风险控制

10.1 要求

风险是普遍、动态存在的，在某一特定环境、特定时间段存在发生的可能性。因此，应随时跟踪、监控风险的变化。

10.2 风险监控

动态跟踪、监控风险发展和变化，是实施风险评估和处理后，应采取的必要的措施，包括：

a）跟踪、监控已识别风险的变化。已处理的已识别风险，其存在的环境、条件和影响等，是否会发生变化，风险应对措施是否合理、适宜，是否存在残余风险等；

b）管理或业务变更后的风险监控。当管理机制、业务（流程、处理等）、技术手段等及相应资源增加、变更后，可能产生新的风险，或引发已识别风险、残余风险发生的可能性。应重新识别、评估可能的风险，并采取相应的应对措施。

10.3 个人信息安全管理体系内审

风险控制，是易于遗漏的风险管理过程，个人信息安全管理体系内审是保证风险控制的重要机制（参见 DB21/T1628.5 第 14 章》）。

10.4 文档管理

应重视风险管理过程中文档的形成和管理，包括：

a）风险管理计划和方案：

1）风险管理目标；

2）风险管理范围；

3）风险管理周期；

4）风险管理责任人职能；

5）风险管理实施安排等。

c）风险评估流程：

1）风险评估目标；

2）风险评估方法；

3）风险评估过程；

3）风险评估依据；

4）风险评估职责等。

d）资源风险识别清单：

1）资源名称、描述、类型、管理部门/责任人；

2）风险类型、描述、来源、等级和影响；

3）风险应对措施等。

e）风险管理报告：总结风险评估和风险处理情况；报告风险管理结果。

f）风险监控报告：

1）已识别风险、残余风险的跟踪、监控情况；

2）资源、业务增加、变更的风险监控；

3）风险监控周期；

4）风险监控处理结果等。

注1：文档管理，参见 DB21/T1628.4《信息安全 个人信息管理文档管理指南》。

参 考 文 献

[1] GB/T 23694-2009 风险管理 术语
[2]GB/T24353-2009 风险管理原则与实施指南