ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX.4—XXXX

信息安全技术 数据安全评价 第4部分：评价指标

Information Security technology-data security evaluation part4：evaluation index

（征求意见稿）

（本草案完成时间：2023-1-10）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是DB21/T XXXX《信息安全技术 数据安全评价》的第4部分。DB21/T XXXX已经发布了以下部分：

——信息安全技术 数据安全评价 第1部分：要求
——信息安全技术 数据安全评价 第2部分：管理指南
——信息安全技术 数据安全评价 第3部分：审核员管理
——信息安全技术 数据安全评价 第4部分：评价指标
——信息安全技术 数据安全评价 第5部分：评价方法
——信息安全技术 数据安全评价 第6部分：资格审核
——信息安全技术 数据安全评价 第7部分：现场管理
——信息安全技术 数据安全评价 第8部分：保证方法
——信息安全技术 数据安全评价 第9部分：仲裁管理
——信息安全技术 数据安全评价 第10部分：审批管理
——信息安全技术 数据安全评价 第11部分：资格管理

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中共辽宁省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：大连软信咨询服务有限公司、国家计算机网络应急技术处理协调中心辽宁分中心、大连交通大学、大连理工现代工程检测有限公司、大连软件行业协会、大连市计算机学会。

本文件主要起草人：郎庆斌、李凯、才昊、孙鹏、尹宏、秦健、宋悦、杨莉、司丹、孙毅、曹剑、王小庚、王鑫。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市和平区光荣街26号甲，联系电话：024-81680033

本文件起草单位通讯地址：大连市高新园区火炬路32号创业大厦A座5层，联系电话：0411-83655207

信息安全技术 数据安全评价 第4部分：评价指标

1 范围

本文件规定了数据安全评价评价的指标体系、评价指标和权重等的规则。

本文件适用于各类数据安全评价机构，亦为已建立数据（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

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件，仅该日期对应的版本适用于本文件；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 XXXX 信息安全技术 个人信息安全 术语

DB21/T 1628.1 信息安全技术 个人信息安全 第1部分：要求

DB21/T 1628.2 信息安全技术 个人信息安全 第2部分：实施指南

DB21/T XXXX 信息安全技术 数据管理规范

DB21/T XXXX.1 信息安全技术 数据安全评价 第1部分：要求

DB21/T XXXX.2 信息安全技术 数据安全评价 第2部分：管理指南

3 术语和定义

DB21/T XXXX、DB21/T XXXX、 DB21/T XXXX.1界定的术语和定义适用于本文件。

4 要求

本文件遵循DB21/T XXXX.1确立的DSE的基本原则和要求，重点描述和指导DSE的评价指标设计的基本规则。

DSE的评价指标设计，应遵循DB21/T 1628系列、DB21/T XXXX标准的基本规则。

DSE的评价指标设计，应基于DB21/TXXXX.1和本文件的基本规则，并参照DB21/T XXXX.n系列其它标准。

DSE的评价指标设计，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认证指标的设计规则。

5 指标体系

5.1 要求

评价机构应依据DB21/T XXXX.1，根据不同的DSE申请者的特征，设计并建立DSE的指标体系。

5.2 构成

5.2.1 图示

DSE指标体系结构，如图1示。

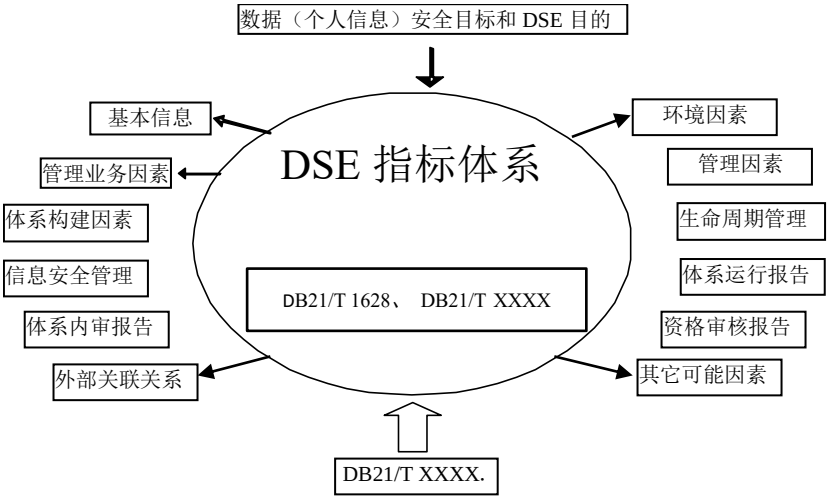


图1　DSE 指标体系结构

5.2.2　要素

设计、建立DSE指标体系应考虑的要素，主要应包括：

a)　数据（个人信息）安全相关法规、标准；
b)　数据（个人信息）安全目标和 DSE 目的；
c)　数据（个人信息）管理者的组织、管理、业务特征；
d)　数据（个人信息）管理者的环境（包括工作环境）特征；
e)　数据（个人信息）管理者内部个人信息的分布、关联因素；
f)　数据（个人信息）管理活动、行为和变化；
g)　DSMS（PISMS）的构建、实施和运行；
h)　DSMS（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)　数据（个人信息管理者）与外部的关联和影响等。

5.2.3　基准

设计DSE指标体系的基准，主要应包括：

a)　数据（个人信息）安全相关法规；
b)　DB21/T 1628 系列标准；
c)　DB21/T XXXX（数据）标准；
d)　DB21/T XXXX 系列标准；
e)　合理、适用的数据（个人信息）管理者的规章制度等。

5.2.4　指标约束

依据DB21/T 2702.1，设计PISMSE指标，应：

a)　客观、真实地反映数据（个人信息）管理者的实际；
b)　设计 DSE 指标项应可操作、可控制。

5.2.5　控制

应考虑DSE指标设计可能存在的偏差，并在审核过程中控制、修正。

5.2.6 评估

应依据DB21/T XXXX.1，评估DSE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) DSE 指标体系与数据（个人信息）安全相关法规、标准的符合性；
b) DSE 指标体系与数据（个人信息）管理者实际的符合性；
c) DSE 指标、指标项的合理性、针对性；
d) DSE 指标偏差的控制和修正；
e) DSE 结果与评价指标间的契合度；
f) DSE 指标体系的持续改进等。

6 评价指标

6.1 关联因素

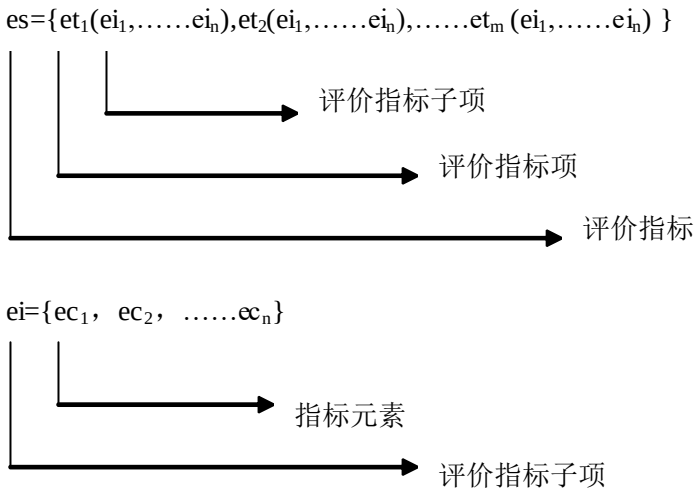
依据DB21/T XXXX.1和DB21/T XXXX.2，DSE指标设计应考虑多种因素间的关联关系：

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 DSMS（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、评估数据（个人信息）管理者内部管理层、执行层等各层级的数据（个人信息）管理状况；
f) DSMS（PISMS）：应全面、整体评估、判断 DSMS（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 DSMS（PISMS）。

6.2 指标构成

6.2.1 构成

DSE指标构成如图2示：



[a] m，n=1，2，……

图2　DSE 指标构成

6.2.2　构成要素

6.2.2.1　评价指标项

依据DB21/T XXXX.1和DB21/T XXXX.2，DSE指标项主要应包括：

a)　管理机制：数据（个人信息）管理的主要要素；
b)　风险管理：数据（个人信息）管理、DSMS（PISMS）安全风险评估；
c)　数据库：数据存储、个人信息数据库的构成机制、管理机制；
d)　数据（个人信息）生命周期：生命周期全过程的管理策略；
e)　安全机制：信息安全技术；
f)　过程管理：基于生命周期的管理策略等。

6.2.2.2　指标子项

依据DB21/T XXXX.1和DB21/T XXXX.2，DSE指标子项主要应包括：

a)　管理机制：主要应包括组织结构、管理计划、管理策略、管理制度、体系建立、文档管理等；
b)　风险管理：主要应包括风险源识别、风险处理和应对等；
c)　数据库：主要应包括管理策略、管理机制、数据库事务等；
d)　数据（个人信息）生命周期：主要应包括数据（个人信息）获取、处理、使用、利用过程的管理策略；
e)　安全机制：ISMS 的相关技术和管理；
f)　过程管理：体系内审、改进、完善等。

6.2.2.3　指标元素

构成DSE指标子项的元素设计，应依据DB21/T XXXX.1和DB21/T XXXX.2，并根据数据（个人信息）管理者的实际、资格审核报告等确定。

6.2.2.4　示例

DSE指标示例，参看附录A。

6.3 改进

应定期评估DSE指标的科学性、合理性、可用性和有效性，持续改进、完善。

7 权重

7.1 要求

DSE指标确定后，应根据数据（个人信息）管理者实际、资格审核报告等确定每个评价指标的权重。

7.2 设计

7.2.1 关联因素

DSE指标的权重设计，应考虑以下因素：

a) 数据（个人信息）管理者的实际需求；
b) DSE 指标的合理性；
c) DSE 指标与数据（个人信息）管理者实际需求的关系等。

7.2.2 方法

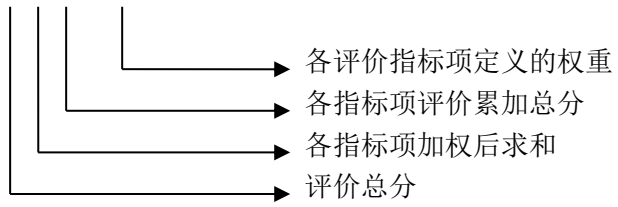
应根据DSE指标相对于数据（个人信息）管理者实际需求的重要性，相互比较确定每个评价指标的权重。权重的设计方法，应包括：

a) 资格审核结果：基于资格审核结果，根据经验、知识、业务评估等确定；
b) DSE 指标分级：根据数据（个人信息）管理者实际确定 DSE 指标的重要程度，据此分级确定；
c) 现场审核修正：基于审核组现场调查修正 DSE 指标权重等。

7.3 加权

DSE各个评价指标项应累加总分加权计算获得评价总分：

$$E=\sum Vet\times Wet$$



7.4 改进

应采取现场随时评估和事后定期评估方式，改进、完善权重设计和权重设计方法。

附 录 A
（资料性）
DSE 指标示例

et	ei	ec	评分
管理机构	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（参照DB21/T 1628.5）	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	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	

DSE指标示例（续）

et	ei	ec	评分
	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	
数据（个人信息）主体权利	管理活动	涉及数据（个人信息）的各种活动、行为、文档的权利保障	
		涉及数据（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	涉及数据（个人信息）相关业务的权利保障方式、策略	
		现场调查	
数据（个人信息）管理者（参照DB21/T 1628.1、DB21/T XXXX）	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	符合标准规定的规则	
		具有管理职能和服务能力	
		现场调查	
管理活动	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	
	环境	环境的安全性	
		移动环境的安全性	
		现场调查	

DSE指标示例（续）

et	ei	ec	评分
数据存储、个人信息数据库（参照DB21/T 1628.3）	识别	数据存储、个人信息分布	
		数据（个人信息）存储、保存形式	
		数据（个人信息）相关记录	
		数据（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	
	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	
	开发	目的、权利、责任	
		方式方法	
		安全保障	
		现场调查	
获取过程	……	……	
处理过程	……	……	
利用过程	……	……	
……	……	……	
过程管理	……	……	
……	……	……	