ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

信息安全技术 网络安全审查规范

Information security technology—specification for network security review

（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。

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：大连软件行业协会、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、大连软信咨询服务有限公司、大连市计算机学会。

本文件主要起草人：郎庆斌、李凯、才昊、尹宏、秦健、宋悦、杨莉、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

引　　言

《数据安全法》、《网络安全法》、《网络安全审查办法》等法规相继发布实施，推进信息安全的秩序建设。法规为纲，以纲为范，标准为目，纲举目张。因此需要研制相应标准，延展法规规则，与法规规则相互救济，规范秩序体系建设。

本文件与《网络安全审查办法》相互引证，并参照DB21/T 2082《信息安全检查规范》，规范网络安全审查的要素、过程、流程等。

信息安全技术 网络安全审查规范

1 范围

本文件规定了网络安全审查要素、管理、流程及过程管理等相关要求。

本文件适用于：

a) 实施网络安全审查的相关组织；

b) 可为网络安全相关运营者、产品或服务提供者提供参考。

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。

《网络安全审查办法》

GB/T 5271.8 信息技术 词汇 第8部分：安全

DB21/T 1799.1 信息技术 信息服务管理规范 第1部分：总则

DB21/T 2082.1 信息安全检查规范 第1部分：管理规范

DB21/T 2082.2 信息安全检查规范 第2部分：技术规范

DB21/T XXXX 信息安全技术 网络安全框架

3 术语和定义

GB/T 5271.8和DB21/T 2082界定的术语和定义适用于本文件。

4 要求

DB21/T 2082规范了信息系统安全检查的基本规则，可为网络安全审查提供参照；

DB21/T XXXX可与DB21/T 2082相互引证、参考。

5 综述

网络安全审查应是基于风险管理驱动的网络安全相关产品、设备、服务及相关活动和行为的评估、审查， 提供基于信息安全相关法规、标准的行为准则：

a) 网络安全审查是系统相关的，DB21/T XXXX 确立的网络安全框架构成要素相互关联、作用和影响，需要系统、整体评估、审查；

b) 网络安全是业务相关的，应基于 DB21/T XXXX 确立的网络安全框架制定适合组织发展目标和业务流程的网络安全审查计划；

c) 网络安全是环境相关的，应在网络安全审查中，基于信息安全总体架构识别网络安全与外部环境之间的安全风险；

d) 网络安全的核心是人，应基于 DB21/T XXXX 确立的规则审查网络安全相关的管理机制、方法、策略、体系；
e) 应遵从《网络安全审查办法》规范的网络安全风险的审查规则等。

6 要素

6.1 内容

基于《网络安全审查办法》、DB21/T XXXX，网络安全审查要素主要应包括网络安全框架构成要素、产品（设备）和相关服务等。

6.2 构成要素

6.2.1 网络

依据DB21/T XXXX，网络构成要素主要应包括：
a) 实体环境：网络运行相关的物理环境要素，包括场地、线路、监控等；
b) 基础平台：支撑网络应用的系统要素，参见 DB21/T XXXX10.2；
c) 内容：网络空间中以各种形态存在的内容，参见 DB21/T XXXX 第 6 章；
d) 应用：基于网络系统的各种相关业务应用、控制软件，如电子政务、电子商务、智能监控、工控系统、物联网等；
e) 传输通道：网络空间内容的传输通道；
f) 接入：各种网络接入形式、终端等；
g) 运行：网络运行状态；
h) 管理：网络的管理形态；
i) 服务：为网络提供的服务形态；
j) 行为和伦理：网络空间的行为模式和应遵守的普遍认同的道德观念、标准等。

6.2.2 网络安全

网络安全构成要素，是基于网络的构成要素形成的，主要应包括：
a) 网络构成要素的安全特征；
b) 网络构成要素间的关联关系；
c) 网络互联、网络与外部环境交互之间的关联关系和安全特征（网络空间边界形态）；
d) 网络拓扑结构的风险特征等。

6.2.3 网络安全审查

基于网络安全框架，网络安全审查要素主要应包括：
a) 网络构成要素的风险评估；
b) 网络安全构成要素的安全性评估；
c) 网络的空间环境安全性评估等。

6.3 产品（设备）

6.3.1 产品分类

网络相关产品（设备）主要应包括：

a) 实体产品（设备）：网络运行相关物理环境相关的产品（设备），包括场地（产品）设备、布线系统、门禁监控系统、运维系统等；
b) 基础产品（设备）：支撑网络及相关系统运行的基础设施，包括网络设备、处理和传输设备、数据（内容）存储设备、安全设备、接入终端等及相关技术；
c) 系统平台产品：支撑网络应用的系统软件，包括网络操作系统、终端操作系统、数据库系统、中间件、云平台、支撑软件、安全系统等及相关技术；
d) 应用产品：基于网络的解决各种实际问题的应用软件。包括科学计算、数据处理、知识获取、事物处理、辅助设计、业务管理等及相关开发技术；
e) 工控系统：支撑工业生产、制造系统运行的自动控制系统相关产品（设备），包括数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）、远程测控单元（RTU）、制造执行系统（MES）、企业资源管理系统（ERP）及传感/监视/ 控制/诊断系统等；
f) 智能产品（设备）：智能采集、智能识别等智能应用产品（设备），包括自动驾驶系统、面部识别系统、各种场景机器人应用等及相关技术等。

6.3.2 网络安全

产品（设备）相关的网络安全要素，主要应包括：
a) 独立产品（设备）的风险、安全特征；
b) 产品（设备）互联的风险、安全特征；
c) 产品（设备）应用的风险、安全特征；
d) 非国产化产品（设备）的远期风险；
e) 产品（设备）供应链的安全特征和风险；
f) 产品（设备）技术支持能力风险等。

6.3.3 网络安全审查

网络相关产品（服务）的安全审查要素，主要应包括：
a) 产品（设备）相关的网络安全要素的风险评估；
b) 基于产品（设备）相关的网络安全要素的产品（设备）安全审查；
c) 网络安全产品（设备）、系统的安全评估；
d) 产品（设备）相关检测、测试、试验等的风险、安全评估；
e) 产品（设备）承载能力、可靠性、健壮性评估等。

6.4 服务

6.4.1 分类

基于网络提供的信息服务分类，参考DB21/T 1799.1。

6.4.2 安全要素

参考DB21/T XXXX第16章，基于网络提供的信息服务的安全要素，主要应包括：
a) 网络相关服务咨询的潜在风险评估；
b) 网络相关服务提供的方式、技术、能力、管理、关联因素等的风险、安全评估；
c) 网络相关服务交付成果物内容的潜在、远期安全评估；
d) 网络相关服务支持的方式、技术、能力、管理、资源、业务融合和连续性等的风险和安全评估；
e) 网络相关服务过程的安全性评估等。

6.4.3 网络安全审查

网络相关服务的安全审查要素，主要应包括：

a) 网络相关服务安全要素的风险、安全评估；
b) 网络相关服务提供者的知识、能力、行为伦理的安全评估；
c) 网络相关服务被提供者的知识、能力、管理等的安全评估；
d) 网络相关服务的物理环境、技术环境、管理环境及其它关联因素的风险、安全评估等。

7 管理

7.1 要求

网络安全审查应建立相应的管理机制， 统一、规范、科学、系统地展开网络安全相关的各项审查工作。

7.2 机构

网络安全审查应组建相应的管理机构，明确管理职能，统一管理网络安全审查的组织、实施、评估、复检等项工作。管理机构的职能主要应包括：

a) 理解网络安全的重大意义，明确网络安全审查的目的；
b) 提供利于网络安全审查的管理平台，有序推进网络安全审查相关工作；
c) 组建网络安全审查机构，为推进、实施网络安全审查提供、组织所需资源支持，包括人员、资金、信息、管理、环境等；
d) 遴选具有信息安全相关知识、能力、专业等的管理、审查人员，保证网络安全审查实施；
e) 对网络安全审查管理过程中可能出现的各种不利因素提供管理决策；
f) 为网络安全审查提供法规、政策指导和决策；
g) 审批网络安全审查报告；
h) 颁发网络安全审查相关资质等。

7.3 机制

网络安全审查管理机构应建立相应的管理机制：

a) 应明确工作制度，确定管理机构的目标；
b) 应依据工作制度建立相应的工作机制、管理流程；
c) 应明确网络安全审查组织、实施的各项职能；
d) 应明确管理机构相关成员的产生机制、工作职责等；
e) 应明确管理机构相关管理、审查人员的职责和义务等。

7.4 宣传培训

网络安全审查管理机构应依据《网络安全审查办法》和本文件，宣传网络安全、信息安全的重要意义和网络安全审查的必要性，保证网络安全相关工作的有序展开。

网络安全审查管理机构应建立网络安全、信息安全相关的培训教育制度，对管理、审查人员及面向社会开展网络安全审查相关的能力培训、教育。

7.5 文档管理

应在网络安全审查组织、实施、评估、复检等过程中记录与网络安全审查相关活动和行为的所有相关信息，并建立与网络安全审查相关的文档备案管理制度。

8 流程

8.1 申请

依据《网络安全审查办法》和本标准，网络安全审查申请者应提交网络安全审查申请书。网络安全审查申请书内容主要应包括：

a) 网络安全审查申请者的合法、合规说明；
b) 网络安全审查相关要素说明；
c) 网络安全审查内容的业务相关性；
d) 网络安全审查相关要素自我评价说明；
e) 网络安全审查相关要素安全缺陷、事故及解决方案等说明；
f) 提交网络安全审查文档材料清单；
g) 其它需要说明的问题等。

8.2 资格审查

8.2.1 要求

网络安全审查应审查网络安全审查申请者的资格，主要应包括申请资格审查和文档材料完整性审查。

8.2.2 申请资格审查

管理机构受理网络安全审查申请者的网络安全审查申请后，应依据网络安全相关法规、标准等和本文件，审核网络安全审查申请者的申请资格。审查内容主要应包括：

a) 网络安全审查申请者的合法性；
b) 网络安全审查申请者申请审查事项的真实性、可信性；
c) 网络安全审查申请者的管理能力评估；
d) 网络安全审查申请者的安全环境评估等。

8.2.3 文档完整性审查

8.2.3.1 文档清单

网络安全审查申请者应提交文档材料，主要应包括：

a) 申请审查事项的说明；
b) 申请审查事项相关的安全风险评估报告；
c) 申请审查事项相关的安全影响评估报告；
d) 申请审查事项相关的各类文档材料，如产品、服务等的采购、验收、工程等文件；
e) 依据《网络安全审查办法》提供相应的安全承诺书；
f) 网络安全审查申请者的各种相关管理文档；
g) 审查事项相关的安全缺陷、事故及解决方案等的详细说明；
h) 网络安全审查相关要素的自我评价说明；
i) 其它需要提供的文档；

j） 其它需要说明的问题等。

8.2.3.2 审查

网络安全审查申请者提交文档的完整性审查，主要应包括：

a） 评估文档、文档内容的规范性、完整性；
b） 评估文档的真实性、有效性；
c） 质疑可能存在的问题，并明确结果等。

8.2.4 报告

网络安全审查的申请资格审查结束应形成相应的报告，主要内容应包括：

a） 网络安全审查申请者的合法性说明；
b） 网络安全审查申请者提交文档材料的规范性、完整性说明；
c） 网络安全审查申请者提交文档材料内容的真实性、有效性说明；
d） 相关评估结果的说明；
e） 存在的缺陷和整改结果的说明；
f） 其它需要说明的问题等。

8.3 审查机制

8.3.1 要求

通过网络安全审查资格审查后，管理机构应建立相应的审查机制，实时审核网络安全审查申请者的申请审查事项。

8.3.2 机构

管理机构应组建网络安全审查机构：

a） 遴选具有信息安全相关知识、能力、专业等的管理、审查人员构成；
b） 明确网络安全审查机构的功能构成、业务分工；
c） 明确网络安全审查机构的职能；
d） 明确网络安全审查机构人员构成的职责；
e） 规范网络安全审查基准、流程、管理、评估等。

8.3.3 秩序

网络安全审查机构应建立规范的网络安全审查秩序：

a） 确立明确的网络安全审查目标；
b） 明确清晰的网络安全审查策略；
c） 规范科学的网络安全审查流程；
d） 规范网络安全审查人员的行为规则；
e） 建立网络安全审查相关风险评估机制；
f） 建立网络安全审查相关规章制度；
g） 建立网络安全审查过程管理机制；
h） 建立争端解决仲裁机制；
i） 建立网络安全审查回溯、评估、学习机制等。

8.3.4 审查体系

网络安全审查应体系化：

a) 根据网络安全审查要素需求，明确网络安全审查要素和目标；
b) 确立网络安全审查管理规则；
c) 确立网络安全审查相关人员管理规则；
d) 明确网络安全审查方式、方法、手段；
e) 建立适用的网络安全审查指标；
f) 建立适用的网络安全审查流程；
g) 规范的网络安全审查过程管理；
h) 规范、科学的网络安全审查质量管理；
i) 规范、科学的网络安全审查评估管理等。

8.3.5 审查指标

网络安全审查机构应基于相关法律、《网络安全审查办法》、DB21/T 2082和本文件，并根据不同的网络安全审查要素需求，设计、建立网络安全审查指标：

a) 应全面、整体评估、判断网络安全审查要素相关的基础、条件、应用场景、关联因素等；
b) 应基于网络安全审查要素的实际需求，真实、客观、准确地反映网络安全审查申请者的实际状况；
c) 网络安全审查指标应考虑网络安全审查申请者的特殊需求等。

8.3.6 人员管理

8.3.6.1 分类

网络安全审查相关人员，主要应包括：

a) 管理人员：主要包括相关机构、相关培训教育、相关咨询组织等的管理人员；
b) 专业人员：主要包括网络安全审查、网络（信息）安全相关咨询、网络（信息）安全相关培训教育及其它网络（信息）安全相关人士等专业技术人员等。

8.3.6.2 管理

网络安全审查相关人员管理，主要应包括：

a) 网络安全审查相关人员的聘任、考核、培训、监督等；
b) 网络安全审查人员相关活动、行为、能力、业绩等的管理、评估；
c) 网络安全审查人员执业资格管理等。

8.3.6.3 职业规范

网络安全审查人员应遵守职业规范：

a) 应在国家法规、《网络安全审查办法》、相关标准框架内，独立、客观、公正、科学、规范地行使网络安全审查职能；
b) 应修正、提高职业操守和执业能力，适应不同工作环境的能力需求；
c) 无法律要求或网络安全申请者的书面授权，应对网络安全审查相关的任何信息保密；
d) 不应传播可能损害网络安全审查相关双方利益的虚假或误导性信息；
e) 不应接受任何网络安全审查申请者相关人员或任何利益相关方的任何馈赠或其它利益输送；
f) 其它必须遵守的职业规范等。

8.3.6.4 基本资格

网络安全审查人员应具备的基本资格，主要应包括：

a) 具备完全民事行为能力；
b) 遵守国家法律，严谨、科学、公正，实事求是，具有良好的职业素养；
c) 具有一定的职业、专业教育经历，具备网络（信息）安全相关专业知识及相关专业知识等专业素质和完成审查必须的基本技能；
d) 取得网络安全审查相关的执业资格；
e) 网络安全审查相关的其它规定等。

8.4 审核

8.4.1 要求

为客观、真实的反映网络安全审查要素的安全特征和基本状况，网络安全审核应包括文档审核和现场审核。

8.4.2 文档审核

应基于国家法规、《网络安全审查办法》、相关标准和本文件，审查网络安全审查申请者提交的相关文档：

a) 审阅、评估网络安全审查相关文档的真实性、有效性；
b) 评估、确认网络安全审查要素相关基础、条件、应用场景的的安全性；
c) 评估网络安全审查要素相关安全风险评估的方法、策略及完整性、有效性；
d) 评估网络安全审查要素相关安全影响评估的边界、范畴、方法、关联因素等及完整性、有效性；
e) 评估、明确网络安全审查申请者各种相关管理的过程方法及规范性、有效性；
f) 评估、确认网络安全审查相关要素相应的安全承诺的真实性、可靠性、有效性和可操作性；
g) 评估、确认网络安全审查要素相关安全缺陷、事故等的解决方案、应急方案的有效性、实用性；
h) 明确需网络安全审查现场审核确认的问题；
i) 需要评估、审阅、确认的其它网络安全审查相关事项等。

8.4.3 现场审核

应基于国家法规、《网络安全审查办法》、相关标准和本文件，实地、现场审核网络安全审查要素的安全特征、基本状况，及文档审核明确的需网络安全审查现场审核确认的问题。

8.4.4 审核报告

网络安全审查文档审核、现场审核结束应形成相应的报告，主要内容应包括：

a) 网络安全审查申请者基本情况说明；
b) 网络安全审查要素安全特征说明；
c) 网络安全审查要素相关基础、环境、条件、应用场景等相关因素说明；
d) 文档审核、现场审核过程说明；
e) 安全缺陷、安全风险、安全影响说明；
f) 网络安全审查相关问题说明、分析；
g) 文档审核、现场审核结论和说明；
h) 建议和意见；
i) 其它需说明的问题等。

8.5 审查报告

网络安全审查结束后应形成网络安全审查报告，主要内容应包括：

a) 网络安全审查申请者基本情况说明；
b) 审核报告；
c) 问题解决说明；
d) 网络安全审查结论及认定方法、过程等的说明；
e) 网络安全风险、影响分析、说明；
f) 网络安全申请者所作网络安全承诺的确认、说明；
g) 网络安全审查要素安全特征的分析、说明；
h) 其它需要说明的问题等。

8.6 审批

网络安全审查结束后，应向相关管理机构提交网络安全审查报告，经相关管理机构审核、批准后颁发网络安全审查相关资质。

8.7 控制

应在网络安全审查流程执行过程中实行管控：

a) 资格审查不能满足网络（信息）安全相关法规标准、《网络安全审查办法》、本文件，应退回网络安全审查申请者，依据审查结果整改，形成整改报告，重新提交审查；
b) 文档审核、现场审核不能满足网络（信息）安全相关法规标准、《网络安全审查办法》、本文件，应退回网络安全审查申请者。依据审核结论整改，形成整改报告，重新提交审核；
c) 网络安全审查结束后如有重大投诉、质疑、争议等，应退回网络安全审查申请者，重新自我评价、针对性整改，并形成整改报告，重新提交申请；
d) 网络安全审查报告审批未获通过，应退回网络安全审查受理机构，重新组织审查等。

8.8 图示

网络安全审查流程如图1示。

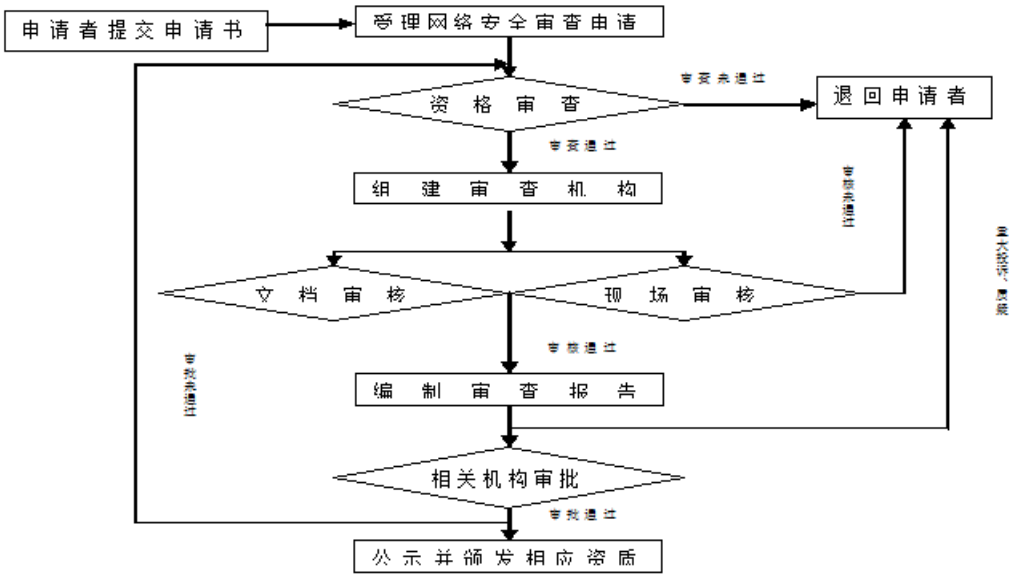

图1 网络安全审查流程

9 过程管理

网络安全审查应实施过程管理，在网络安全审查过程中分析、发现网络安全审查流程的缺陷、问题，随时修正、改进，提高网络安全审查的有效性、权威性。