ICS 91.120.25
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

信息化全过程网络安全服务规范

Cybersecurity service specification for the whole process of informatization

（征求意见稿）

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：北方实验室（沈阳）股份有限公司、辽宁省标准化研究院。

本文件主要起草人：张健楠、韩晓娜、朱江、袁洪朋、李海涛、刘文志、刘兴华、隋大智、李琳、梁爽、高殿悦、丁显东、吴晓峰、马超、牛晓雷、邱学思、叶松 、韩燕妮。

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。

归口管理部门通讯地址：辽宁省工业和信息化厅（沈阳市皇姑区北陵大街45-2号），联系电话：024-86893258。

标准起草单位通讯地址：北方实验室（沈阳）股份有限公司（沈阳市浑南新区三义街6-1号21层），联系电话：024-83785841 / 83785849。

信息化全过程网络安全服务规范

1 范围

本文件规定了信息化全过程网络安全服务的术语和定义、总则、全过程服务组织模式及人员职责、投资决策综合性咨询服务、网络安全设计服务和网络安全专项服务的要求。

本文件适用于辽宁省内信息化全过程网络安全服务的实施

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。

GB/T 18336.2—2015 信息技术 安全技术 信息技术安全性评估准则

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

ISO/IEC 27001 信息技术 安全技术 信息安全管理体系要求

3 术语和定义

GB/T 18336—2015、 GB/T 22239—2019、GB/T 25069—2010、GB/T 25070—2019、GB/T 28448—2019、GB/T 39786—2021和ISO/IEC 27001界定的以及下列术语和定义适用于本文件。

3.1

网络安全服务 cybersecurity service

面向组织或个人的各类网络安全保障需求，由服务提供方按照服务协议所执行的一个网络安全过程或任务。

3.2

安全保护能力 security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

3.3

网络安全设计 cybersecurity design

针对信息系统的安全保障需求，设计总体安全策略，形成安全架构、技术体系和管理体系的设计。

3.4

投资决策咨询 investment decision consultation

在项目前期研究阶段，通过对投资项目的技术、产品、市场、工艺技术及设备、财务效益、内外部发展环境等方面的分析和评价，分析计算投资项目在项目计算期产生的预期现金流确定其投资价值以及相关的风险有多大，进而做出投资决策。

3.5

信息安全管理体系 information security management system

在整体或特定范围内建立信息安全目标和策略，以及完成这些目标和策略所用方法的总集。

3.6

网络安全监理 network security supervision

具有相关资质的监理单位受网络安全工程建设单位的委托，依据国家批准的信息化工程项目建设文件、有关工程建设的法律法规和工程建设监理合同及其他工程建设合同，对乙方的工程建设实施监督的一种专业化服务活动。

3.7

信息安全风险评估 Information security risk assessment

从风险管理角度，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。

3.8

网络安全等级保护测评 testing and evaluation for graded cybersecurity protection

测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密的网络安全等级保护状况进行检测评估的活动。

3.9

商用密码应用安全性评估 security evaluation of commercial cryptography application

指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。

4 基本要求

4.1 总则

信息化全过程分为规划设计、招标采购、部署实施、验收评估、运行维护和绩效评价共六个阶段。

4.2 原则

信息化全过程网络安全服务针对各个阶段的特点，应按以下原则，构建完善的网络安全服务能力体系：

a) 规划设计阶段提供规划及设计等网络安全服务；
b) 招标采购阶段提供招标采购咨询等网络安全服务；
c) 部署实施阶段提供安全监理及项目管理等网络安全服务；
d) 验收评估阶段提供安全风险评估及测评等网络安全服务；
e) 运行维护阶段提供安全运维及应急保障等网络安全服务；
f) 绩效评价阶段提供绩效评价等网络安全服务。

5 服务组织模式及人员职责

5.1 组织模式

5.1.1 服务过程分为规划设计、招标采购、部署实施、验收评估、运行维护和绩效评价六个阶段。

5.1.2 每个阶段对应提供不同的安全服务项，为信息化全过程建设各个阶段的网络安全提供全方位的服务和保障。

5.1.3　全过程网络安全服务内容如图 1 所示：

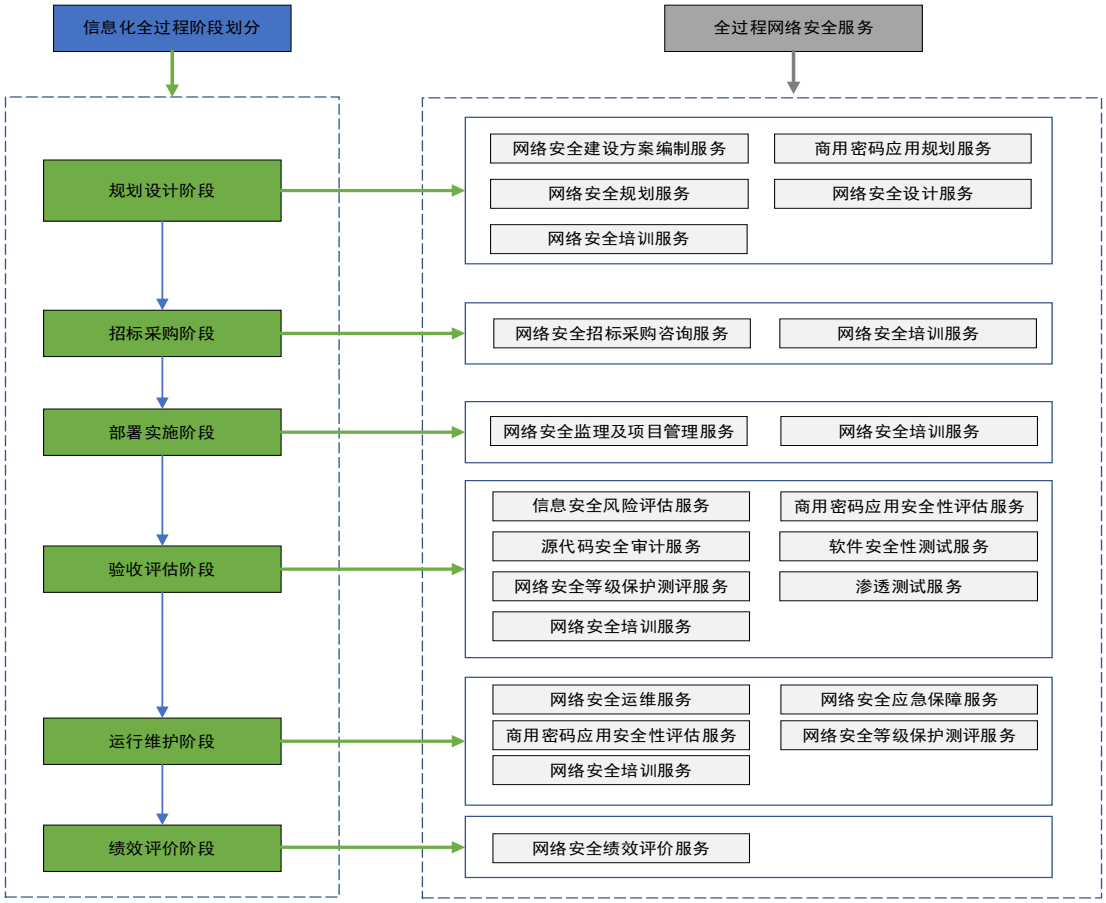

图1　全过程网络安全服务内容图

5.2　人员职责

各岗位人员职责如表1所示：

表1　人员职责划分表

序号	角色	职责
1	全过程网络安全领导组	全面负责组织全过程网络安全服务工作，决策制定、进度把控
2	投资决策综合性咨询服务组	负责制定投资决策综合性咨询服务的服务方案、负责网络安全建设方案编制、负责商用密码应用规划编制
3	网络安全规划师	负责网络安全服务的整体规划
4	网络安全设计师	制定网络安全设计方案
5	网络安全招标采购咨询师	为网络安全服务项目提供采购咨询
6	网络安全监理工程师	编写监理规划中的网络安全管理的监理工作内容及监理实施细则；审查施工单位报送的营业执照、企业资质和安全生产许可证

序号	角色	职责
7	网络安全风险评估师	对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行风险评估
8	等保测评师	负责信息安全服务项目的安全评估工作;负责信息安全服务等级保护项目实施,协助客户完成定级备案、专家评审、差距分析、方案设计、安全整改、管理制度等相关工作
9	密码测评师	对商用密码应用安全性评估工作提供技术支持，并对其项目测评的方法、方案、进度、输出成果等进行把控；对网络安全等级保护测评工作提供技术支持，并对其项目测评的方案、进度输出成果等进行把控
10	渗透测评师	实施网络和 Web、app 的渗透测试；能对常见的漏洞原因、原理、可利用性、风险程度等相关分析报告，如 sql 注入，xss，csrf，命令执行，文件包含，任意文件下载/读取。文件上传，越权/未授权操作等漏洞；对互联网领域的重大安全事件进行跟踪、分析；跟踪最新行业领域技术相关知识输出；对安全领域的新技术、新方法进行研究
11	绩效评价师	组织开展本单位信息化系统建设实施预算绩效管理工作，专注绩效咨询评价、职业能力提升、政策继续教育
12	文档管理员	负责样品、文档保管、交接、跟踪和保密工作
13	计划管理员	负责对外联络，协助领导组开展工作
14	质量保证工程师	负责全过程网络安全服务的质量监督
15	专家	全过程网络安全服务技术咨询

6　6 投资决策综合性咨询服务

6.1　投资决策咨询

投资决策咨询应按以下步骤进行：

a）　确定投资目标，确定投资目标是投资决策的前提；

b）　选择投资方向，在明确投资目标后，应进一步拟定具体的投资方向；

c）　制定投资方案，在决定投资方向之后，应着手制定具体的投资方案，并对方案进行可行性论证；

d）　评价投资方案，主要是对投资风险与回报进行评价分析，由此来断定投资决策方案的可靠性；

e）　反馈调整决策方案和投资后的评价，投资方案确定之后，还必须要根据环境和需要的不断变化，对原先的决策进行适时地调整，从而使投资决策更科学合理。

6.2　网络安全规划编制

网络安全规划应按以下几个方面进行规划：

a）　通过风险评估等方式提取组织的安全需求，对相应的安全保障目标、任务、措施和步骤进行规划；

b） 从策略、组织、管理、技术、资源等多个层面进行规划。

6.3 网络安全建设方案编制

网络安全建设方案可分为三个层面，依据需求逐步完善。

a） 以基础安全技术框架、网络安全管理体系、现有安全风险控制建设为重点；

b） 构建以人机结合分析、持续监测、安全事件流程闭环为核心的主动安全防御体系；

c） 重点完善主动防御体系，以漏洞、资产、威胁、事件四个维度为抓手，建设漏洞管理平台、资产管理平台、威胁实时监测、事件管理平台，形成以安全效果为目标的安全运营体系。

6.4 商用密码应用规划编制

应当做到系统建设与商用密码保护同步规划、同步建设、同步运行，已建重要信息系统密码应用逐步进行改造，整体规划如下：

a） 推进基准站网商用密码应用：摸清基准站商用密码应用需求、制定商用密码应用实施方案、商用密码应用试点示范和推广应用；

b） 推进面向社会服务的商用密码应用；

c） 建立健全商用密码应用标准体系；

d） 加强科技创新，推动商用密码广泛应用。

7 网络安全设计服务

7.1 网络安全设计

7.1.1 基本要求

网络安全设计按照GB/T 25070—2019中第5节安全技术设计框架及第6、7、8、9章不同等级安全保护环境设计要求开展，包括设计总体安全策略、制定网络安全建设方案和实施方案，并在此基础上形成安全架构、技术体系和管理体系的设计。

网络安全设计一般可分为顶层设计、初步设计和详细设计等不同的服务交付物。

网络安全设计还可以包含对网络安全产品的功能和性能设计，以及选型建议。

7.1.2 商用密码应用解决方案编制

商用密码应用解决方案应从技术和管理两个方面的要求进行方案建设：

——技术要求层面：

1） 应从物理和环境安全的角度出发构建方案；

2） 应从网络和通信安全的角度出发构建方案；

3） 应从设备和计算安全的角度出发构建方案；

4） 应从应用和数据安全的角度出发构建方案。

——管理要求层面：

1） 应从管理制度的角度出发构建方案；

2） 应从人员管理的角度出发构建方案；

3） 应从建设运行的角度出发构建方案；

4） 应从应急处置的角度出发构建方案。

7.1.3 信息安全管理体系建设

信息安全管理体系建设主要是依照国际或国家信息安全管理体系相关标准（ISO/IEC 27001），应按以下原则进行建设：

a) 确定信息安全管理体系范围，包括影响其实现信息安全管理体系预期结果能力的外部和内部事项、与信息安全相关的要求、相应接口及依赖关系；
b) 制定信息安全方针包括信息安全目标、对满足适用的信息安全相关要求的承诺、对持续改进信息安全管理体系的承诺；
c) 明确管理职责，最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通；
d) 以风险评估为基础选择控制目标与控制方式，量化测评风险发生的可能程度及其造成的后果；
e) 制定程序文件阐述被保护的资产、组织风险管理的方法、控制目标及控制方式和需要的保证程度。

7.2 网络安全招标采购咨询

7.2.1 招投标文件及合同咨询

网络安全招标采购咨询主要包括以下内容：

a) 提供网络安全领域项目招标文件编制和招标技术的咨询指导服务，协助完成详细的具体的技术质量要求的技术性文书；
b) 提供网络安全领域项目投标文件编制和投标技术的咨询指导服务，协助完成应招标文件要求编制的技术响应性文件；
c) 提供网络安全领域项目招投标合同的咨询指导服务，协助完成招标合同中的技术内容。

7.3 网络安全监理及项目管理服务

7.3.1 网络安全监理

网络安全监理主要包括以下内容：

a) 依据网络安全方面的标准和要求，在工程建设各阶段向建设单位提供相关咨询,并协助建设单位对承建单位在工程建设中的网络安全实施服务，实施控制和管理；
b) 对信息系统运维阶段的其他网络安全实施服务进行监理。

7.3.2 网络安全项目管理

可提供的网络安全项目管理服务包括：范围管理、项目风险管理、项目集成管理、质量管理、时间管理、项目人力资源管理、工程咨询服务、综合能力管理、采购管理、成本管理、沟通管理等。

8 网络安全专项服务

8.1 信息安全风险评估服务

信息安全风险评估按照GB/T 18336.2—2015中第6章执行，具体评估流程如下：

a) 风险评估准备，制定评估工作计划，包括评估业务范围、评估标准内容等；
b) 资产识别，确定资产的机密性、完整性和可用性，进行资产赋值，并对重要和关键资产进行标注；
c) 威胁识别，进行威胁识别、威胁分类和威胁赋值；
d) 脆弱性识别，进行脆弱性识别和脆弱性赋值；
e) 已有安全措施确认，应确认安全措施的有效性；

f） 风险分析，风险分析及风险值计算，形成风险评估报告。

8.2 网络安全等级保护测评服务

网络安全等级保护测评按照GB/T 22239—2019中第6、7、8、9章执行，及GB/T 28448—2019中第6、7、8、9章不同级别安全测评要求开展，具体测评流程如下：

a） 测评准备，信息收集和分析、工具和表单准备；
b） 测评方案编制，确定测评对象、测评指标、测评内容、工具及测评方法；
c） 现场测评，进行现场测评和结果记录、结果确认和资料归还；
d） 形成测评报告，进行单项测评结果判定、单元测评结果判定、整体测评、系统安全评估、安全问题风险分析，形成等级测评结论并编制测评报告。

8.3 商用密码应用安全性评估服务

商用密码应用安全性评估依据GB/T 39786—2021中第5章通用要求及第6、7、8、9章不同级别系统密码应用基本要求开展，具体评估流程如下：

a） 评估密码应用方案，编制测评方案，包括密码应用解决方案、实施方案和应急处置方案；
b） 前期准备，搜集系统部署图等文档证据、人员访谈了解系统业务情况；
c） 现场测评，进行工具测试和人工核查；
d） 进行密码应用安全评估并根据系统的密码应用情况出具测评报告。

8.4 软件安全性测试服务

8.4.1 软件安全性测试包括程序、网络、数据库安全性测试。

——程序安全性测试：

1） 测试是否明确区分系统中不同用户权限；
2） 测试系统中会不会出现用户冲突；
3） 测试用户登陆密码是否是可见、可复制；
4） 测试是否可以通过绝对途径登陆系统；
5） 测试用户退出系统后是否删除了所有鉴权标记，是否可以使用后退键而不通过输入口令进入系统。

——网络安全性测试：

1） 测试采取的防护措施是否正确装配好，有关系统的补丁是否及时修补；
2） 模拟非授权攻击，查看防护系统是否坚固；
3） 采用成熟的网络漏洞检查工具检查系统相关漏洞；
4） 采用各种木马检查工具检查系统木马情况；
5） 采用各种防外挂工具检查系统各组程序的客外挂漏洞。

——数据库安全性测试：

1） 测试系统数据的机密性；
2） 测试系统数据的完整性；
3） 测试系统数据可管理性；
4） 测试系统数据的独立性；
5） 测试系统数据可备份和恢复能力。

8.4.2 通过对程序、网络、数据库安全性测试，对软件进行安全评估，并根据软件实际情况出具测评报告。

8.5 源代码安全审计服务

源代码安全审计服务主要包括以下内容：

a) 通过自动化代码安全扫描工具，对源代码进行非破坏性质的审计工作；
b) 通过工具扫描、手工测试验证相结合的方法，对源代码进行非破坏性质的审计工作；
c) 通过对业务系统模块的源代码进行审查，检查代码在程序编写上可能引起的安全性和脆弱性问题；
d) 通过对源代码进行安全审计，根据软件实际安全性和脆弱性问题出具测评报告。

8.6 网络安全运维服务

网络安全运维服务包括以下内容：

a) 安全巡检，通过定期安全巡检（工具扫描及安全专家人工检测）检查设备（网络架构，网络设备，服务器主机，操作系统，数据库和用户账号，口令等安全对象）是否存在不安全因素；
b) 安全加固，对操作系统和数据库系统进行安全配置加固，网路及安全设备安全加固；
c) 补丁管理，针对客户补丁管理提供的建议，帮助客户维护补丁管理系统和防病毒系统；
d) 应急响应及安全通告，定期通过邮件或者其他联系方式向客户提供系统的安全通告，为客户实时提供最新的安全漏洞和安全警告，可使客户提高尽快速处理突发事件的能力，保证客户信息系统的安全。

8.7 渗透测试服务

渗透测试应按以下流程开展：

a) 信息收集：通过公开渠道、直接访问、扫描网站等方式获取目标信息；
b) 漏洞探测：完成信息收集之后，对网站进行漏洞探测；
c) 漏洞验证：将探测到的有可能成功利用的全部漏洞逐一进行验证，验证成功后再应用于目标中；
d) 权限提升：利用目标系统存在的弱点进行本地权限提升并直接控制目标系统；
e) 内网渗透：通过模拟攻击外网服务器，获取外网服务器的权限，利用外网服务器作为跳板，攻击内网其他服务器，获取有用信息和数据；
f) 信息整理：整理渗透工具、整理收集信息、整理漏洞信息；
g) 报告输出：进行整理资料，对漏洞成因、验证过程和带来危害进行分析，并提出修补建议，对所有产生的问题提出合理高效安全的解决办法。完成渗透测试报告编写；
h) 痕迹清理：可用 MSF 中的 clearev 命令清除痕迹、清除 mstsc 痕迹、清除 web 日志文件等。

8.8 网络安全应急保障服务

网络安全应急保障服务包括以下内容：

a) 网络环境安全事件的应急处置：对火灾、盗窃、破坏等紧急事件按照国家消防、公安有关法律法规的有关规定处理。影响网络运行和信息安全的重大事件由应急处置工作组统一指挥处置；
b) 网络运行事件处置：网络运行相关事件由网络部负责，重大事件立即向应急处置工作组负责人报告；
c) 网络攻击事件处置：由网络部按应急流程处置，对于大规模、影响较大的恶意代码、拒绝服务攻击、系统入侵和端口扫描进行处置；

d) 信息安全事件处置：发生信息安全事件应及时通知网络部安全负责人，及时消除非法信息，恢复系统；
e) 应急演练：根据组织已有的应急预案，在设备、系统、业务、组织等不同层面进行测试和演练,从而提高组织的应对各类突发网络安全事件的能力，演练的方式可分为桌面演练、模拟演练和实战演练。

8.9 网络安全培训服务

网络安全培训服务包括以下内容：

a) 基础培训：包括安全导论、安全法律法规、操作系统应用、计算机网络、HTML&JS、PHP 编程、Python 编程、docker 基础等；
b) web 安全培训：包括 web 安全概述、web 安全基础、web 安全漏洞及防御、企业 web 安全防护策略等；
c) 渗透测试培训：包括渗透测试概述、渗透测试环境搭建、渗透测试工具使用、信息收集与社工技巧、web 渗透、中间件渗透、内网渗透等；
d) 代码审计培训：包括代码审计概述、PHP 代码审计、Python 代码审计、Java 代码审计、C/C++ 代码审计、代码审计实战等；
e) 安全加固培训：包括网络协议安全、密码学及应用、操作系统安全配置等；
f) 企业级培训：包括企业安全建设、等保原理、等保制度建设、等保测评实践等。

8.10 网络安全绩效评价服务

从网络安全管理的效力,效率两方面对组织的网络安全管理水平进行评价。确定各评价指标的权重，得出效力、效率两个维度的评价值以及综合评价结果。实现从定性到定量的综合集成，为管理者提供比较客观、准确的评价结果。