ICS 35.240
CCS A 90

DB3601

南 昌 市 地 方 标 准

DB3601/11—2024

数字化项目网络安全审查规范

Cybersecurity review specification of digital projects

2024-06-03 发布　　2024-09-01 实施

南昌市市场监督管理局　　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。

本文件由南昌市互联网信息办公室提出并归口。

本文件起草单位：南昌市互联网信息办公室、江西安极信息技术有限公司。

本文件主要起草人：周凡、宋徽青、张伦芳、肖慧、武永伟、周围、刘煜、潘伟琦、何琪、黄瑞。

数字化项目网络安全审查规范

1 范围

本文件规定了数字化项目（非涉密）网络安全审查的审查方式、审查流程、审查内容、审查结果。

本文件适用于数字化项目（非涉密）规划设计阶段的网络安全审查，其他信息化项目网络安全审查可参照执行。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

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 35273 信息安全技术 个人信息安全规范

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 40692 政务信息系统定义和范围

DA/T 28 建设项目档案管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字化项目 Digital projects

全市各级行政机关以及法律法规授权的具有管理公共事务职能的组织等使用财政性资金建设、运维的数字化项目，主要包括：电子政务网络平台、重点业务数字化系统、数据资源库、信息安全基础设施、电子政务基础设施（政务云、数据中心等）、数字政府标准化体系以及相关支撑体系等符合《政务信息系统定义和范围》（GB/T 40692）规定的非涉密项目。

[来源：江西省数字化项目建设管理办法，1,2,有修改]

3.2

项目设计方案 Project design scheme

在项目建设过程中编制的可行性研究报告、初步设计方案、深化设计方案、投资概算或项目建议书等。

3.3

安全设计方案 Security design scheme

项目设计方案中包含的网络安全体系总体设计方案、商用密码应用方案、数据安全保护方案等子方案。

3.4

关键信息基础设施 Critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：关键信息基础设施安全保护条例，1,2]

3.5

网络安全投入 Cybersecurity investment

项目建设及运行过程中投入的安全咨询服务、安全运维服务、安全技术服务、安全集成服务、等保测评服务、商用密码安全性评估服务、安全软件、安全设备及其他硬件等相关费用。

3.6

建设单位 Constructing units

对项目实施进行组织管理，并在项目建设过程中负总责的部门。

[来源：DA/T 28]

3.7

审查部门 Review department

负责组织网络安全审查工作的部门。

4 审查方式

建设单位应向审查部门提交审查材料，审查部门开展审查工作并出具审查意见。

5 审查流程

5.1 总体流程

应参照数字化项目网络安全审查流程执行（数字化项目网络安全审查流程图见附录A）。

5.2 审查申报

建设单位应提交项目设计方案等书面审查材料。

5.3 审查受理

审查部门收到审查材料后应受理审查并通知建设单位。

5.4 开展审查工作

5.4.1 审查工作分为初步审查和专家审查，初步审查为审查部门就申报材料进行初步审查，给出初步审查意见；专家审查为审查部门聘请专家进行审查，要求建设单位配合审查工作。

5.4.2 专家审查工作应由不低于三名专家组成的专家组负责，设置一名专家组组长。流程主要分为三步，一是建设单位陈述申报建设项目安全设计方案等相关情况，二是专家组针对审查疑问进行提问，三是专家组讨论并形成专家意见和建议。

5.5 问题整改

审查部门给出书面的审查结果后，建设单位应针对审查结果中的相应条款进行必要的安全整改工作并书面报送审查部门。

5.6 审查意见

审查部门应出具审查意见并反馈给建设单位。

6 审查内容

应参照数字化项目网络安全审查细则执行（数字化项目网络安全审查细则见附录B）。

7 审查结果

审查结果应分“通过”和“不通过”两种情况：

——审查结果为“通过”时，项目可按项目设计方案进行建设；

——审查结果为“不通过”时，建设单位应对提交的项目设计方案进行修改并重新提交审查。

应参照数字化项目网络安全审查结果判别说明确定审查结果（参见附录C）。

附 录 A
（规范性）
数字化项目网络安全审查流程图

图 A.1 规定了数字化项目网络安全审查流程。

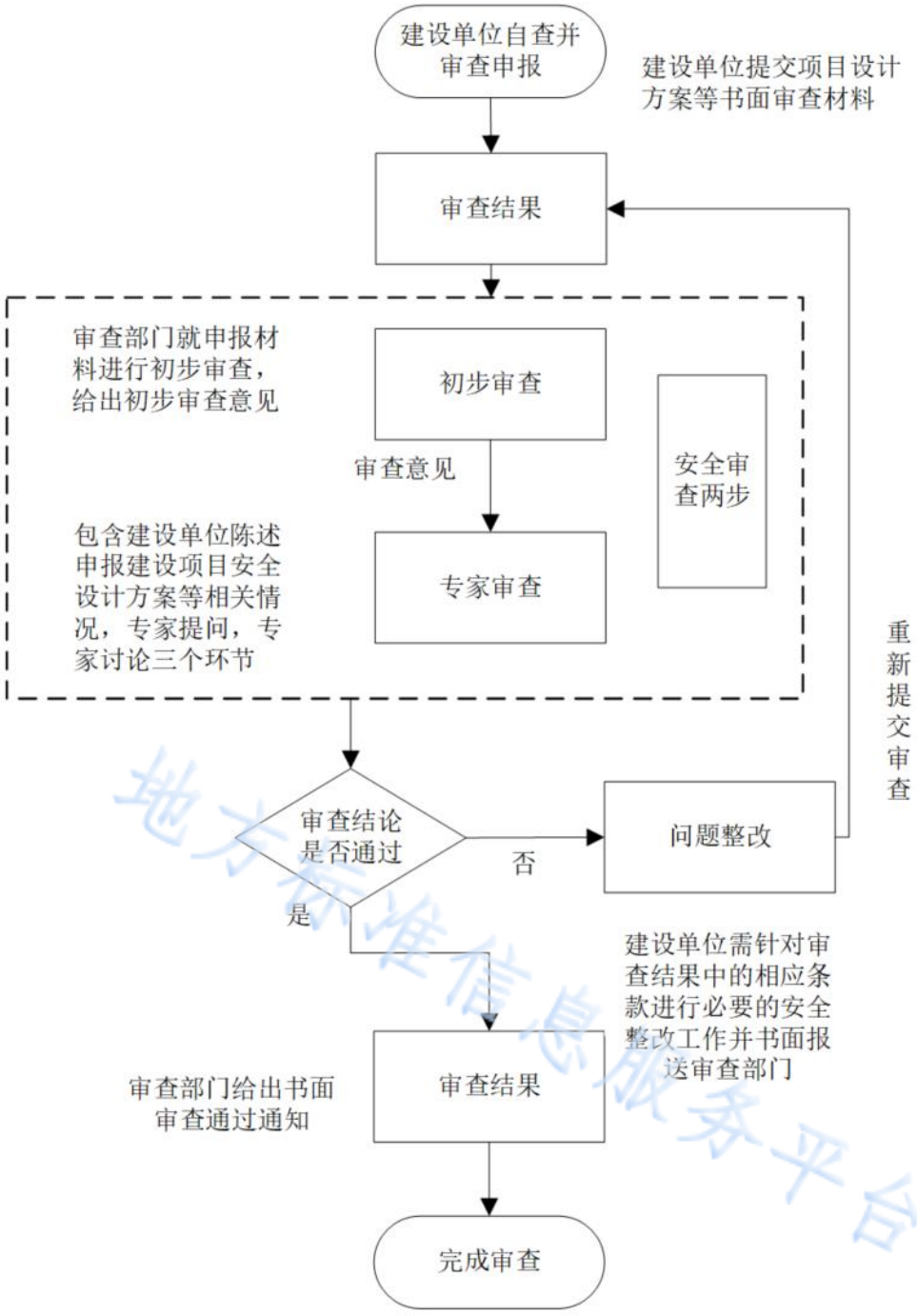

图 A.1 数字化项目网络安全审查流程

附 录 B
（规范性）
数字化项目网络安全审查细则

表 B.1 规定了数字化项目网络安全审查细则。

表 B.1 数字化项目网络安全审查细则

序号	审查方向	审查指标	审查内容		审查方法	审查内容要求
1	安全规划设计	网络安全目标、保护对象等设计的合理性，包括是否列为关键信息基础设施。	项目设计方案中应明确网络安全目标、保护对象，保护设计思路，针对设计给出合理依据。		查阅项目设计方案及相关材料，是否具备审查要求的内容	建议项
			项目设计方案中应明确建设项目（系统）是否列为关键信息基础设施。			必须项
2		保护对象的网络安全保护等级自定级情况及确定理由。	项目设计方案中应给出建设项目（系统）的保护等级，给出等级确定的依据，依据必须严格按照《GBT 22240 信息安全技术 网络安全等级保护定级指南》要求，部分行业可结合行业定级要求综合评定。		查阅项目设计方案及相关材料，是否具备审查要求的内容	必须项
3		网络安全现状及风险分析。根据安全保护等级的要求对网络安全设备和系统现状、网络安全管理现状及网络安全风险等进行分析，并依据现状及风险分析提出安全设计需求。	项目设计方案中应明确阐述当前安全现状、现状应从多个角度进行阐述，包括但不仅限于：物理环境、通信网络、区域边界、业务应用、商用密码应用、计算环境、安全管理等现状及管理机构、管理人员、建设管理、运维管理等网络安全管理制度方面。		查阅项目设计方案及相关材料，是否具备审查要求的内容	建议项
			明确以上网络安全现状下每个方面的安全设计需求。			建议项
4	安全防护设计	安全规划及安全方案设计的合理性。根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计。针对性地提出物理环境、网络架构、边界防护、计算环境、安全管理、商用密码应用安全	物理环境安全	位置应选择在防震、抗风、防雨的建筑内。	查阅项目设计方案及相关材料，是否具备审查要求的内容，部分内容可提供承诺书	必须项
				具备物理访问控制、防盗窃和防破坏、防雷击、防火、防水防潮、防静电、温湿度控制，短期的备用电力供应等要求。		必须项
				应在设置自动消防系统的基础之上对机房划分区域进行管理，区域和区域之间设置隔离防火措施。（等级保护定级为三级及以上要求）。		必须项
				应规划设置冗余或并行的电力电缆线路为计算机系统供电。（等级保护定级为三级及以上要求）。		必须项
				上云系统需要云环境通过等级保护测评，应保证云计算基础设施位于中国境内。		必须项
			物理安全说明：依据建设项目业务系统实际放置位置（如			

表 B.1　数字化项目网络安全审查细则（续表）

序号	审查方向	审查指标	审查内容		审查方法	审查内容要求
		等相关防护措施。	自建机房、公有云、政务云、混合模式）情况确定物理实际安全要求，在非自建机房的情况下，部分要求内容可能不适用，如建设单位使用政务云部署业务系统，仅需要提供政务云通过等级保护证明即可。			
			通信网络安全	网络架构应按照分区分域原则进行设计。		必须项
				应针对通信线路、关键网络设备和关键计算设备进行冗余设计，保障系统可用性。（等级保护定级为三级及以上要求）。		必须项
				应采用密码技术保证通信过程中数据完整性和保密性。		必须项
				应针对重要网络区域与其他网络区域之间采取技术隔离手段。（等级保护定级为三级及以上要求）		必须项
			安全区域边界	应在区域边界采取访问控制或隔离技术手段。		必须项
				应在网络边界采取检测、防止攻击行为的技术措施。		必须项
				应在网络边界对用户的行为和重要安全事件进行审计。		必须项
				应对远程接入用户的行为进行单独的审计。（等级保护定级为三级及以上要求）。		必须项
				应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。（等级保护定级为三级及以上要求）。		必须项
			安全计算环境	进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听。		必须项
				应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。		必须项
				应建立备份机制，对重要数据处理系统进行数据备份或热备，信息系统根据系统重要性应建设相应级别备份系统。		必须项
			安全管理中心	应对网络中的运维管理行为进行身份鉴别，应能对运维管理行为进行安全审计。		必须项
				应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。（等级保护定级为三级及以上要求）。		必须项
				应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间不少于六个月。		必须项
				应对网络链路、安全设备、网络设备和服务器等的		必须项

表 B.1　数字化项目网络安全审查细则（续表）

序号	审查方向	审查指标	审查内容		审查方法	审查内容要求
				运行状况进行集中监测。（等级保护定级为三级及以上要求）。		
			密码应用安全	法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护。（等级保护定级为三级及以上要求）。		必须项
				根据商用密码应用需求，制定商用密码应用方案，规划商用密码安全保障。（等级保护定级为三级及以上要求）。		必须项
				自行或者委托商用密码检测机构开展商用密码应用安全性评估。（等级保护定级为三级及以上要求）。		必须项
5	数据安全设计	数据安全设计的合理性。涉及数据资源建设的，是否对重要业务信息、系统数据及软件系统进行识别。是否根据数据的重要性和数据对系统运行的影响，制定数据备份策略和恢复策略、备份程序和恢复程序等。	应当按照国家对数据分类分级保护的相关要求对建设项目（系统）中的数据实行分类分级保护，确定建设项目（系统）中的重要数据清单，对列入清单的数据进行重点保护，明确保护措施。		查阅项目设计方案及相关材料，是否具备审查要求的内容，部分内容可提供承诺书	必须项
			制定数据备份或容灾措施，在发生安全问题的时候能够进行有效恢复。			必须项
			明确数据安全审计措施。			必须项
			关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。			必须项
6	预算和产品选型	产品选型的合理性。方案所选用的网络安全产品是否符合国家和主管部门网络安全管理有关规定。	项目设计方案中选用的网络安全设备应提出采购要求，要求后期采购的网络安全设备需按要求通过安全认证或安全检测。		查阅项目设计方案及相关材料，是否具备审查要求的内容，部分内容可提供承诺书	必须项
			项目设计方案中选用的密码产品应提出采购要求，要求后期采购的密码产品需具备国家密码管局局颁发的密码证书。			必须项
7		项目的资金预算及依据，网络安全资金安排计划是否满足国家、省、市有关网络安全管理的相关规定及网络安全保障需求。	新建设项目（系统）的网络安全（含软硬件安全设备、安全运维、安全维保、渗透测试、风险评估、等级保护测评、商用密码应用安全性评估等）预算不低于项目总预算的 5%。		查阅项目设计方案及相关材料，是否具备审查要求的内容，部分内容可提供承诺书	必须项

表 B.1　数字化项目网络安全审查细则（续表）

序号	审查方向	审查指标	审查内容		审查方法	审查内容要求
8	安全管理制度	网络安全管理制度建立情况。确保安全策略、管理制度和操作规程等保障措施同步实施，并保障系统处于持续安全防护状态。	安全管理制度	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	查阅项目设计方案及相关材料，是否具备审查要求的内容，部分内容可提供承诺书	建议项
				应形成由安全策略、管理制度、操作规程，记录表单等构成的全面的安全管理制度体系。（等级保护定级为三级及以上要求）。		必须项
				安全管理制度应通过正式、有效的方式发布，并进行版本控制，制度按照需求进行修订。		必须项
			安全管理机构	成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。		必须项
				明确管理机构各岗位和职责设置，明确审批流程。		必须项
				应配备专职的安全管理员，不可兼职。（等级保护定级为三级及以上要求）。		必须项
			安全管理人员	完善人员录用流程和要求，明确人员离岗流程。		必须项
				明确外部人员访问管理制度。		必须项
				应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。（等级保护定级为三级及以上要求）。		必须项
			安全建设管理	完善系统定级备案流程和进行安全方案设计。		必须项
				安全方案设计应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。		必须项
				项目建设应全程邀请第三方监理单位监督项目的实施全过程。（等级保护定级为三级及以上要求）。		必须项
			安全运维管理	按照要求定期开展网络安全检测、风险评估、等级保护测评工作。		必须项
				应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资金保障、事后教育和培训等内容。		必须项
				应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等。		必须项
				应定期对系统相关的人员进行应急预案培训，并进行应急预案演练，并定期对原有的应急预案重新评估，修订完善。（等级保护定级为三级及以上要求）。		必须项
9	国产化要	国产化要求和供应链安全	项目设计方案中所选用的安全类产品原则上应为国产，因业务需要使用国外产品的需明确阐述使用理由。		查阅项目设计方案及相	建议项

表 B.1　数字化项目网络安全审查细则（续表）

序号	审查方向	审查指标	审查内容	审查方法	审查内容要求
	求和供应链安全		项目设计方案中选用的安全产品、安全服务应提出采购要求，要求后期提供方与建设单位签订保密协议和网络安全责任书。	关材料，是否具备审查要求的内容	必须项
			项目设计方案中选用的安全产品、安全服务应提出采购要求，要求后期提供方提供技术服务人员提供背景审查材料。		必须项

附 录 C
（规范性）
数字化项目网络安全审查结果判别说明

C.1 数字化项目网络安全审查结果为“通过”的要求

数字化项目网络安全审查细则中的审查内容要求“必须项”和“建议项”都满足的判定为“通过”。

C.2 数字化项目网络安全审查结果为“不通过”的要求

有下列情况之一判定为“不通过”。

a）网络安全保障体系未进行系统化、结构化设计，安全防护层面缺失较大；
b）产品与服务采购不符合国家相关规定；
c）项目建设参考安全技术标准为老旧标准；
d）其他结合实际情况应判定为“不通过”的情况。

参 考 文 献

[1] 中华人民共和国网络安全法
[2] 中华人民共和国密码法
[3] 中华人民共和国数据安全法
[4] 中华人民共和国个人信息保护法
[5] 网络安全审查办法
[6] 关键信息基础设施安全保护条例
[7] 互联网政务应用安全管理规定
[8] 江西省人民政府办公厅关于印发《江西省数字化项目建设管理办法》的通知 （赣府厅发〔2023〕12 号）
[9] 南昌市人民政府办公厅关于印发《南昌市政务信息化项目集约化建设管理办法》的通知（洪府厅发〔2020〕126 号）