ICS 35.040
CCS L 80

DB2101/T

沈 阳 市 地 方 标 准

DB2101/T 0030—2021

网络安全管理评估规范

Specifications for network security management assessment

2021-07-01 发布　　2021-08-01 实施

沈阳市市场监督管理局　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。

本文件由中共沈阳市委网络安全和信息化委员会办公室提出并归口，同时负责标准的宣贯、监督实施等工作。

本文件起草单位：东软集团股份有限公司、东北大学、辽宁省信息安全与软件测评认证中心、沈阳赛宝科技服务有限公司、沈阳欣欣晶智计算机安全检测技术有限公司。

本文件主要起草人：张泉、陈静相、路娜、王华铎、葛长龙、杨菲菲、周福才、郭剑锋、赵英科、金鑫、纪德海、文军日、金玉平。

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、来函等方式进行反馈，我们将及时答复并认真处理，根据实施情况依法进行评估及复审。

本文件归口部门联系电话：024-22821200；联系地址：沈阳市浑南区沈中大街 206-1 号。

本文件起草单位联系电话：18640508881；联系地址：沈阳市浑南新区新秀街 2 号。

引　言

为落实《中华人民共和国网络安全法》相关要求，解决地区产业结构差异、地区性共性及有代表性的个性化网络安全问题，通过制定《网络安全管理评估规范》标准，规范有关部门开展网络安全评估工作，充分掌握各级关键行业网络运营者的安全风险和防护状况。制定本标准旨在以查促建、促管、促改、促防，最终推动关键行业网络运营者安全责任制和网络安全防范体系的建立和落实，保障关键行业信息系统安全稳定运行。

《网络安全管理评估规范》列出了网络运营者在网络安全评估方面的流程、程序，定义了评估的主要内容。

评估流程分为工作准备、工作实施和结果反馈三个阶段，其中工作准备阶段是对评估实施有效性的保证，是评估工作的开始；工作实施阶段是对评估活动中涉及的评估内容进行判定，同时基于获得的各类信息进行关联分析，计算风险值，并综合评估整体安全状况出具评估报告；结果反馈阶段是对评估实施质量判定的过程，是评估工作的终止。

评估程序是围绕评估工作的全生命周期，根据不同阶段的工作事项，为达到相应评估目的应采取的手段和行为方式，用于规范和指导评估者开展和落实网络安全评估具体工作。

评估内容主要包括法律法规合规、行业领域要求、安全管理措施、安全技术措施、技术检测等方面的评估，通过文档查阅、现场访谈等方法，检查被评估方是否遵从法律、法规和政策标准的相关要求，是否存在安全漏洞和安全隐患。

网络安全管理评估规范

1 范围

本文件给出了网络安全评估工作的评估流程、评估程序和评估内容。

本文件适用于有关部门开展网络安全评估工作参考；网络运营者自行开展网络安全评估工作参考；网络安全服务机构对网络运营者提供咨询、检测、评估等服务参考；网络安全检测产品及服务研发机构研发检查工具、安全咨询服务、创新安全应用参考。

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。

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 25069 中界定的以及下列术语和定义适用于本文件。

3.1

网络运营者 Network operators

网络的所有者、管理者和网络服务提供者。

4 缩略语

下列缩略语适用于本文件。

IP：互联网协议（Internet Protocol）

MAC：介质访问控制（Medium Access Control）

5 评估流程

网络安全评估应根据图1所示的工作准备阶段、工作实施阶段和结果反馈阶段3个阶段开展评估实施工作。

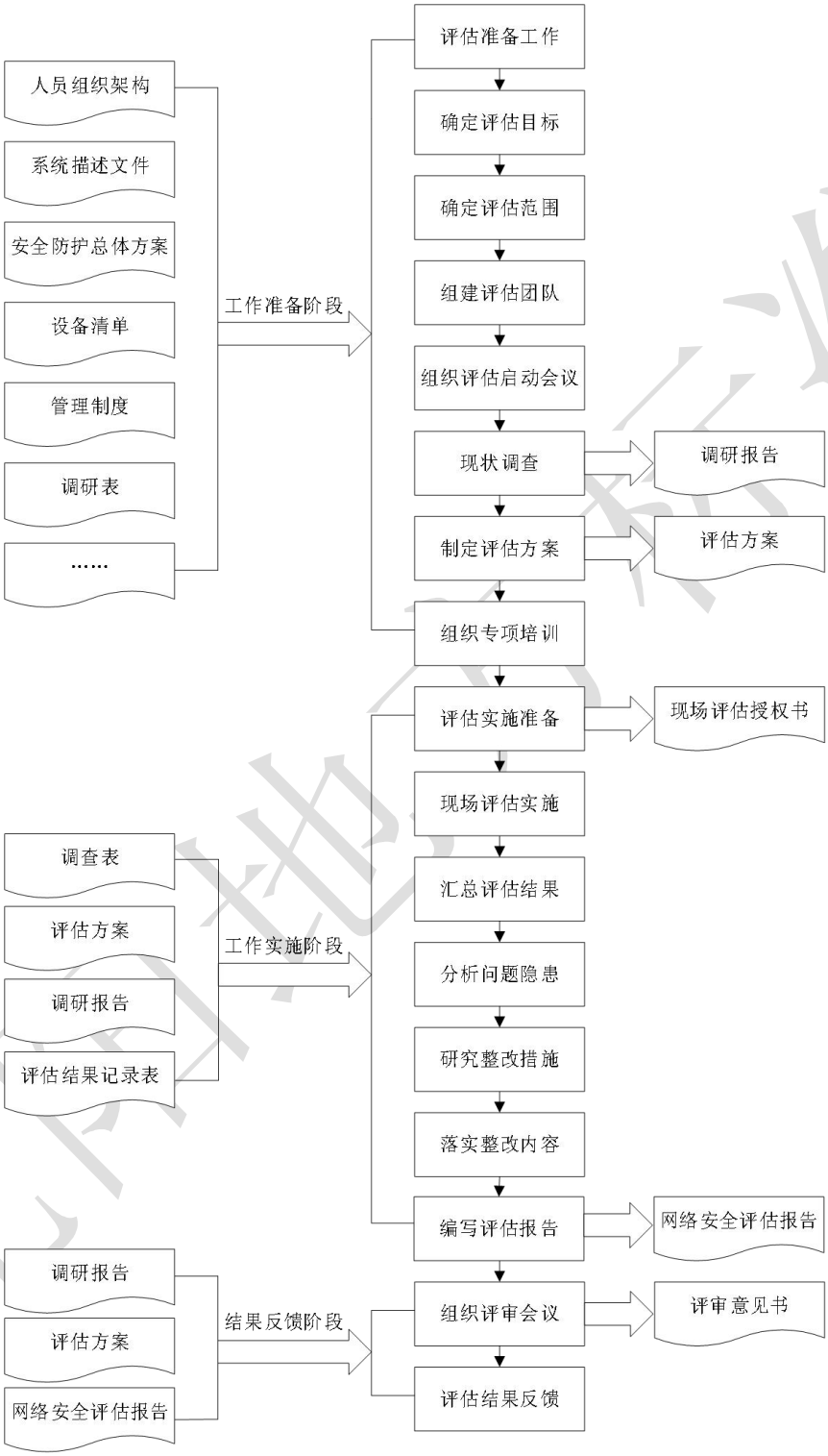

图 1 网络安全评估实施流程

6 评估程序

6.1 工作准备阶段

6.1.1 评估准备工作

评估方应明确评估的背景、原则和依据，充分调研被评估方所属行业的相关标准及政策文件，确定评估工作任务。

评估方应按照国家相关要求做好保密工作，与被评估方签署保密协议，明确问责和追责等处理方法，保证评估过程中产生、接触的所有记录、数据评估结果的安全、保密，并适情签署个人保密协议。

6.1.2 确定评估目标

评估方应根据以下内容确定评估的目标：

a） 网络安全评估的目标应根据满足组织业务持续发展在安全方面的需要、法律法规的规定等内容来明确网络安全评估目标；

b） 网络安全评估应根据当前信息系统的实际情况来确定在信息系统生命周期中所处的阶段，并以此来明确网络安全评估目标。

6.1.3 确定评估范围

评估方应结合已确定的评估目标和组织的实际情况，合理定义评估对象和评估范围边界。评估范围的边界划分依据应包括但不限于以下内容：

a） 业务系统的业务逻辑边界；

b） 网络及设备载体的边界；

c） 物理环境边界；

d） 组织管理权限边界；

e） 其他。

6.1.4 组建评估团队

网络安全评估工作应根据图2所示的内容组建评估团队。

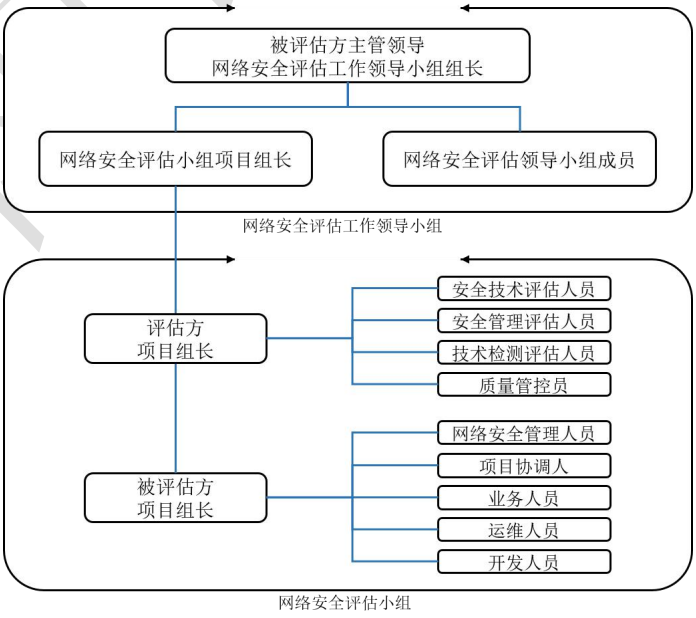

图 2 网络安全评估团队框架

网络安全评估工作领导小组应由被评估方主管信息化或网络安全工作的领导、相关业务部门领导以及评估方项目组长等人员组成。网络安全评估工作领导小组主要负责决策网络安全评估工作的目的、目标；参与并指导网络安全评估准备阶段的启动会议；协调评估实施过程中的各项资源；组织评估项目验收会议；推进并监督风险处理工作等。

网络安全评估小组应由评估方、被评估方等共同组建，必要时可聘请相关专业的技术专家进行技术支持。网络安全评估小组主要负责完成评估前的表格、文档、检测工具等各项准备工作；进行网络安全评估技术培训和保密教育；制定网络安全评估过程管理相关规定；编制应急预案等。

网络安全评估小组应采用合理的项目管理机制，主要相关成员角色与职责说明如表1和表2所示。

表 1 网络安全评估小组——评估方构成角色与职责说明

评估方 人员角色	工作职责
项目组长	网络安全评估项目中实施方的管理者、责任人。具体工作职责包括： 1） 根据项目情况组建评估项目实施团队； 2） 根据项目情况与被评估方一起确定评估目标和评估范围，并组织项目组成员对被评估方实施系统调研； 3） 根据评估目标、评估范围及系统调研的情况确定评估依据，并组织编写评估方案； 4） 组织项目组成员开展网络安全评估各阶段的工作，并对实施过程进行监督、协调和控制，确保各阶段工作的有效实施； 5） 与被评估方进行及时有效的沟通，及时商讨项目进展状况及可能发生问题的预测等； 6） 组织项目组成员将网络安全评估各阶段的工作成果进行汇总，编写《网络安全评估报告》等项目成果物； 7） 负责将项目成果物移交被评估方，向被评估方汇报项目成果，并提请项目验收。
安全技术 评估人员	网络安全评估项目中技术方面评估工作的实施人员。具体工作职责包括： 1） 根据确定的评估目标与评估范围参与系统调研，并编写《调研报告》的技术部分内容； 2） 参与编写《评估方案》； 3） 遵照《评估方案》实施各阶段具体的技术性评估工作，主要包括：信息资产调查、行业领域要求检查、安全技术措施检查等； 4） 对评估工作中遇到的问题及时向项目组长汇报，并提出需要协调的资源； 5） 将各阶段的技术性评估工作成果进行汇总，参与编写《网络安全评估报告》等项目成果物； 6） 负责向被评估方解答项目成果物中有关技术性细节问题。
安全管理 评估人员	网络评估项目中管理方面评估工作的实施人员。具体工作职责包括： 1） 根据评估目标与评估范围的确定参与系统调研，并编写《调研报告》的管理部分内容； 2） 参与编写《评估方案》； 3） 遵照《评估方案》实施各阶段具体的管理性评估工作，主要包括：信息资产调查、法律法规合规检查、行业领域要求检查、安全管理措施检查等； 4） 对评估工作中遇到的问题及时向项目组长汇报，并提出需要协调的资源； 5） 将各阶段的管理性评估工作成果进行汇总，参与编写《网络安全评估报告》等项目成果物； 6） 负责向被评估方解答项目成果物中有关管理性细节问题。
技术检测 评估人员	网络评估项目中技术检测评估工作的实施人员。具体工作职责包括： 1） 根据评估目标与评估范围的确定参与系统调研，并编写《调研报告》的技术检测部分内容； 2） 参与编写《评估方案》；

表 1 网络安全评估小组——评估方构成角色与职责说明（续）

评估方 人员角色	工作职责
技术检测 评估人员	3） 遵照《评估方案》实施各阶段具体的技术检测评估工作，主要包括：信息资产调查、渗透测试、漏洞扫描等； 4） 对评估工作中遇到的问题及时向项目组长汇报，并提出需要协调的资源； 5） 将各阶段的技术检测评估工作成果进行汇总，参与编写《网络安全评估报告》等项目成果物； 6） 负责向被评估方解答项目成果物中有关技术检测细节问题。
质量管控员	网络安全评估项目中质量管理的人员。具体工作职责包括： 1） 监督审计各阶段工作的实施进度与时间进度，对可能出现的影响项目进度的问题及时通告项目组长； 2） 负责对项目文档进行管控。

表 2 网络安全评估小组——被评估方构成角色与职责说明

被评估方 人员角色	工作职责
项目组长	网络安全评估项目中被评估方的管理者。具体工作职责包括： 1） 与评估方的项目组长进行工作协调； 2） 组织本单位的项目组成员在网络安全评估各阶段活动中的配合工作； 3） 组织本单位的项目组成员对项目过程中实施方提交的评估信息、数据及文档资料等进行确认，对出现的偏离及时纠正； 4） 组织本单位的项目组成员对评估方提交的《网络安全评估报告》等项目成果物进行审阅； 5） 组织对网络安全评估项目进行验收； 6） 可授权项目协调人负责各阶段性工作，代理实施自己的职责。
网络安全 管理人员	被评估方的专职网络安全管理人员。在网络安全评估项目中的具体工作职责包括： 1） 在项目组长的安排下,配合评估机构在网络安全评估各阶段中的工作； 2） 参与对评估机构提交的《评估方案》进行研讨； 3） 参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认,及时指正出现的偏离； 4） 参与对评估机构提交的《网络安全评估报告》等项目成果物进行审阅； 5） 参与对网络安全评估项目的验收。
项目协调人	网络安全评估项目中被评估方的工作协调人员。具体工作职责是负责与被评估方各级部门之间的信息沟通,及时协调、调动相关部门的资源,包括工作场地、物资、人员等,以保障项目的顺利开展。
业务人员	被评估方的业务使用人员代表(应由各业务部门负责人或其授权人员担任)。在网络安全评估项目中的具体工作职责包括: 1） 在项目组长的安排下,配合评估机构在网络安全评估各阶段中的工作； 2） 参与对评估机构提交的《评估方案》进行研讨； 3） 参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认,及时指正出现的偏离； 4） 参与对评估机构提交的《网络安全评估报告》等项目成果物进行审阅； 5） 参与对网络安全评估项目的验收。
运维人员	被评估方的信息系统运行维护人员。在网络安全评估项目中的具体工作职责包括: 1） 在项目组长的安排下,配合评估机构在网络安全评估各阶段中的工作； 2） 参与对评估机构提交的《评估方案》进行研讨；

表 2 网络安全评估小组——被评估方构成角色与职责说明（续）

被评估方人员角色	工作职责
运维人员	3） 参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认,及时指正出现的偏离； 4） 参与对评估机构提交的《网络安全评估报告》等项目成果物进行审阅； 5） 参与对网络安全评估项目的验收。
开发人员	被评估方本单位或第三方外包商的软件开发人员代表。在网络安全评估项目中的具体工作职责包括: 1） 在项目组长的安排下,配合评估机构在网络安全评估各阶段中的工作； 2） 参与对评估机构提交的《评估方案》进行研讨； 3） 参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认,及时指正出现的偏离； 4） 参与对评估机构提交的《网络安全评估报告》等项目成果物进行审阅； 5） 参与对网络安全评估项目的验收。

6.1.5 组织评估启动会议

网络安全评估领导小组应组织召开网络安全评估工作启动会议，参与人员应该包括评估小组全体人员、相关业务部门主要负责人，如有必要可邀请相关专家组成员参加。启动会议应包括但不限于以下内容：

a） 宣布此次评估工作的意义、目的、目标，以及评估工作中的责任分工；
b） 说明本次评估工作的计划和各阶段工作任务，以及需要配合的具体事项；
c） 介绍评估工作一般性方法和工作内容等。

6.1.6 现状调查

评估方应对被评估方开展现状调查，被评估方提供的信息应包括：

a） 被评估方负责人信息及人员组织架构；
b） 被评估方的网络设备、信息系统等基本信息；
c） 被评估方行业领域相关法律法规、政策文件和标准规范清单；
d） 主要运营业务及其工作流程；
e） 关键岗位从业人员信息；
f） 网络安全管理制度；
g） 安全防护基本情况以及曾发生的网络安全事件情况；
h） 近一年内自行或委托开展检测评估情况、接受有关部门抽查检测情况；
i） 根据实际需要提供其他相关信息。

6.1.7 制定评估方案

评估方应制定网络安全评估方案，并得到被评估方的确认和认可。网络安全评估方案应包括但不限于以下内容：

a） 网络安全评估工作框架：包括评估目标、评估范围、评估依据等；
b） 评估团队组织：包括评估小组成员、组织结构、角色、责任；
c） 评估工作计划：包括各阶段工作内容、工作形式、工作成果等；
d） 风险措施：包括保密协议、评估工作环境要求、评估方法、工具选择、应急预案等；
e） 时间进度安排：评估工作实施的时间进度安排；
f） 项目验收方式：包括验收方式、验收依据、验收结论定义等；

g） 项目管理制度：包括质量管理、风险管理、项目阶段确认书等；
h） 被评估方需要配合的事项清单；
i） 其他。

6.1.8 组织专项培训

评估方应组织专项培训，对负责评估工作的干部、专家、技术人员、有关运维人员等进行广泛培训，确保评估工作质量，培训内容应包括评估目的意义、流程方法、登记表填报说明、网络安全评估方法等。

6.2 工作实施阶段

6.2.1 评估实施准备

评估方应对安全评估实施过程进行风险控制，可采取严格操作的申请和监护、操作时间控制、应急预案制定、运行系统模拟环境搭建、关键业务系统采用人工评估、评估人员选取、评估现场安全培训等风险控制手段，防止安全评估过程中引入的风险。

当评估活动由有关部门发起并委托安全服务机构进行时，评估方应获得该领域业务主管部门的认定或者委托授权，被评估方应当提供评估所必要的软硬件条件和工作环境。

6.2.2 现场评估实施

评估方应按照评估方案的要求，通过文档查阅、现场访谈、现场检查、现场测试4种方法对被评估方所涉及的评估内容实施网络安全评估，并就发现的主要问题与被评估方进行现场签字确认：

a） 文档查阅应包括：查阅被评估方的系统规划设计方案、网络拓扑图、系统安全防护计划、安全策略、架构、要求、标准作业程序、授权协议、系统互连备忘录、网络安全事件应急响应计划等文档，评估其准确性和完整性；
b） 现场访谈应包括：依据评估实施之前准备好访谈问卷或调查表，补充在文档查阅中未被发现的系统细节，进一步理解和洞察系统的开发、集成、供应、使用、管理等过程。现场访谈记录表参见附录A；
c） 现场检查应包括：根据评估方案和评估指导书，在合理的评估环境下，检查各项安全功能和防护能力是否与提交文档一致，是否符合相关标准和要求等；
d） 现场测试应包括：根据评估方案，在被评估单位授权的前提下，运用渗透测试、漏洞扫描等方法直接在待评估系统现场环境上进行安全性测试。

6.2.3 汇总评估结果

评估实施完成后，评估方应及时对评估结果进行梳理、汇总，从安全管理、技术防护等方面对评估发现的问题和隐患进行分类整理。

6.2.4 分析问题隐患

6.2.4.1 关键属性分析

评估方应分析被评估方的业务特点，给出系统对象及相关资产在业务连续性、系统完整性和数据机密性等方面的等级（分为高、中、低三个等级）和具体描述，并把等级为高的系统对象及相关资产的业务特性定义为关键属性，关键属性可以是上述几个特性的组合。系统对象及相关资产的重要性等级应按照GB/T 20984-2007中5.2条款“资产识别”和GB/T 31509-2015中5.2.2条款“资产识别”进行划分，在被评估方的意见基础之上，由评估方确定。

6.2.4.2 脆弱性识别

评估方应根据评估内容的检查结果，对系统对象的脆弱性等级进行分析（高、中、低）并给出具体描述。脆弱性等级应按照GB/T 20984-2007中5.4条款“脆弱性识别”和GB/T 31509-2015中5.2.4条款“脆弱性识别”进行划分，在被评估方的意见基础之上，由评估方确定。

6.2.4.3 威胁分析

评估方应根据检查结果，结合安全威胁清单，根据分析被评估方的业务特点，按照威胁的来源（内部和外部）与威胁发生的可能性，对系统对象进行威胁分析并给出具体描述。威胁分析方法应按照GB/T 20984-2007中5.3条款“威胁识别”和GB/T 31509-2015中5.2.3.4条款“威胁分析”中定义的方法。

6.2.4.4 风险分析评估

评估方应根据关键属性分析、脆弱性分析和威胁分析的结果，对系统对象每个关键属性逐一进行定性风险分析，定性风险分析应按照GB/T 20984-2007中5.6条款“风险分析”中定义的方法（参考附录B的风险分析模型进行风险值的计算），并给出每个关键属性风险分析结果和描述，最后根据风险分析的结果综合评估网络运营者的整体安全状况。

在上述分析评估的基础上，若存在以下情况之一的，应认定该系统对象的网络安全风险为高：

a） 评估内容中有5项及以上高风险的；

b） 网络运营者未发现系统对象已存在公开高危漏洞的，或发现后未采取修补措施或制定修补计划的；

c） 对自查和主管监管部门评估发现的问题和提出的整改意见，有时限要求，但在时限要求内未完成的；无时限要求，在评估结束1个月后未制定整改计划的；

d） 出现2起或以上未对发现或通报预警的网络安全高危漏洞、风险、威胁和事件等及时进行应对或处置，或未按要求反馈情况的；

e） 出现瞒报、漏报、谎报等违反《中华人民共和国网络安全法》相关规定的。

6.2.5 研究整改措施

评估方应根据评估内容中存在的安全风险类型，通过以下4种方式研究提出针对性的安全整改建议：

a） 接受。准备应对风险事件，接受风险的后果，包括积极的开发应急计划；

b） 消减。实施相应的安全措施减少风险发生的概率，包括完善安全管理制度、部署安全产品等；

c） 转移。对风险造成的损失的承担的转移，包括合同的约定，由保证策略或者第三方担保；

d） 规避。通过计划的变更来消除风险或风险发生的条件，包括安全加固、代码完善等。

6.2.6 落实整改内容

被评估方网络安全管理部门应根据评估方的建议，组织相关单位和人员进行整改，安全整改应遵循以下内容：

a） 被认定为关键信息基础设施的，应根据整改意见及时进行安全整改；

b） 应加强对整改效果和整改效率的管理，涉及到大范围整改时，可根据需要委托具有相应安全资质或集成资质的机构进行整改措施的落实；

c） 整改完成后应组织评估方进行再次评估；

d） 对于不能及时整改的内容，应根据风险与责任之间的关系、风险的严重程度，通过风险转移、制定整改计划和时间表进行风险的处置。

6.2.7 编写评估报告

评估方对评估工作进行全面总结，根据评估得到的结果，输出正式的评估报告（模板示例参见附录C），报告应包括但不限于以下内容：

a） 被评估方描述：网络运营单位基本情况、网络拓扑情况、核心资产情况、承载业务情况和安全防护现状；
b） 评估结果说明：评估项、评估内容、评估结果、发现的主要问题（安全漏洞、隐患和被攻击情况等）及其详细描述；
c） 整改情况说明：整改项、整改内容、整改效果、未整改情况及其详细描述；
d） 安全风险分析：通过对评估中发现的安全问题及风险，汇总分析存在的安全隐患及造成的影响；
e） 安全状况评价：结合被评估方所承载业务重要性和威胁，综合评价被评估方的网络安全总体状况。

6.3 结果反馈阶段

6.3.1 组织评审会议

评审会应由被评估方组织，评估方协助，必要时可聘请相关专业的技术专家进行技术支持。评审会议针对评估项目的实施流程、评估的结论、分析的模型与计算方法及评估活动产生的各类文档等内容进行审核，并形成最终材料。评审会议应包括如下内容：

a） 组织人员应提供有关文档供评审人员进行检查，包括但不限于调研报告、评估方案、网络安全评估报告等；
b） 评估项目组长及相关人员应对评估技术路线、工作计划、实施情况、达标情况等内容进行汇报，并解答评审人员的质疑；
c） 评审会中，应由专门记录人员负责对评审会议内容进行记录；
d） 评审结束后，应形成评审结论，并由相关人员进行签字确认；
e） 评估方应将最终材料一并提交被评估方，作为评估项目结束的移交文档。

6.3.2 评估结果反馈

评估方应将评估工作情况和评估报告向委托方（包括被评估方）反馈。

7 评估内容

7.1 法律法规合规评估

7.1.1 关键信息基础设施保护

评估方应根据被评估方的关键业务，查看关键信息基础设施相关材料，检查支撑关键业务的网络设备和信息系统是否均纳入了认定范围，并检查下列内容：

a） 应如实上报支撑关键业务的网络设备和信息系统，避免存在漏报、误报、瞒报的情况；
b） 关键信息基础设施的新建、更新、废弃等流程应符合相关规定；
c） 应开展网络安全等级保护工作，并依据关键信息基础设施法律法规要求实行重点保护，包括安全机构设置、关键人员背景审查、系统和数据容灾备份等；
d） 应自行或者委托网络安全服务机构每年对其网络的安全性和可能存在的风险进行一次检测评估；
e） 应建立健全的网络安全监测预警和信息通报制度,并按照规定报送网络安全监测预警信息；
f） 应满足关键信息基础安全保护相关标准要求。

7.1.2 个人隐私数据保护

评估方应了解被评估方搜集个人隐私数据的目的和范围，并检查下列内容：

a） 应建立个人信息和重要数据保护制度；

b） 应在用户授权范围内或依据相关要求收集、存储、使用数据；

c） 如因业务需要，向境外提供个人信息和重要数据的，应进行安全评估；

d） 应按照GB/T 35273-2020的要求，规范在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为。

7.1.3 网络产品和服务供应链

评估方应检查被评估方采购的网络产品和服务，并检查下列内容：

a） 网络产品、服务应符合相关国家标准的强制性要求；

b） 网络产品、服务正式运行前或发生变更前应通过安全检测并记录；

c） 应与产品和服务的提供者签订安全保密协议，明确安全和保密义务与责任；

d） 对可能影响国家安全的产品或服务，应通过国家安全审查；

e） 应通过采购文件、协议等要求产品和服务提供者配合网络安全审查。

7.1.4 网络安全等级保护

评估方应检查被评估方对等级保护要求的落实情况，例如等级保护定级备案证明、等级保护测评报告等。

7.2 行业领域要求评估

评估方应查看被评估方提供的法律法规、政策文件和标准规范清单，检查被评估方在相关行业领域相关规定、标准的落实情况。

7.3 安全管理措施评估

7.3.1 网络安全组织管理

评估方应检查被评估方网络安全组织管理情况，并检查下列内容：

a） 应明确一名主管领导，负责本单位网络安全管理工作，根据国家法律法规有关要求，结合实际组织制定网络安全管理制度，完善技术防护措施，协调处理重大网络安全事件；

b） 应指定一个机构，具体承担网络安全管理工作，负责组织落实网络安全管理制度和网络安全技术防护措施，开展网络安全教育培训和监督检查等；

c） 应建立健全岗位网络安全责任制度，明确岗位及人员的网络安全责任。

7.3.2 网络安全日常管理

7.3.2.1 基本要求

评估方应检查被评估方网络安全日常管理的基本情况，并检查下列内容：

a） 应制定网络安全工作的总体方针和目标，明确网络安全工作的主要任务和原则；

b） 应建立健全网络安全相关管理制度；

c） 应加强对人员、资产、采购等的安全管理，并保证网络安全工作经费投入。

7.3.2.2 人员管理

评估方应检查被评估方人员管理情况，并检查下列内容：

a） 应与重点岗位的计算机使用和管理人员签订网络安全与保密协议，明确网络安全与保密要求和责任；

b） 应制定并严格执行人员离岗离职网络安全管理规定，人员离岗离职时应终止信息系统访问权限，收回各种软硬件设备及身份证件、门禁卡等，并签署安全保密承诺书；

c） 应建立外部人员访问机房等重要区域审批制度，外部人员须经审批后方可进入，并安排本单位工作人员现场陪同，对访问活动进行记录并留存；

d） 应对网络安全责任事故进行查处，对违反网络安全管理规定的人员给予严肃处理，对造成网络安全事故的依法追究当事人和有关负责人的责任，并以适当方式通报。

7.3.2.3 信息资产管理

评估方应检查被评估方信息资产管理情况，并检查下列内容：

a） 应建立并严格执行信息资产管理制度；

b） 应指定专人负责信息资产管理；

c） 应建立信息资产台账（清单），统一编号、统一标识、统一发放；

d） 应及时记录信息资产状态和使用情况，保证账物相符；

e） 应建立并严格执行设备维修维护和报废管理制度。

7.3.2.4 经费保障

评估方应检查被评估方经费保障情况，并检查下列内容：

a） 应将网络安全设施运行维护、网络安全服务采购 、日常网络安全管理、网络安全教育培训、网络安全检查、网络安全风险评估、网络安全应急处置等费用纳入部门年度经费保障范围；

b） 应严格落实网络安全经费预算，保证网络安全经费投入。

7.3.2.5 采购管理

评估方应检查被评估方采购管理情况，并检查下列内容：

a） 应采购符合相关国家标准的强制性要求的信息技术产品和服务。采购基于新型技术的产品和服务或者国外产品和服务时，应进行必要性和安全性评估；

b） 网络安全产品的采购应符合国家的有关规定；

c） 接受捐赠的信息技术产品，使用前应进行安全测评，并与捐赠方签订信息安全与保密协议；

d） 信息系统数据中心、灾备中心不得设立在境外。

7.3.3 信息系统基本情况

7.3.3.1 基本信息梳理

评估方应查验被评估方的信息系统规划设计方案、安全防护规划设计方案、网络拓扑图等相关文档，访谈信息系统管理人员与工作人员，了解掌握系统基本信息并记录结果。包括：

a） 应掌握主要功能、部署位置、网络拓扑结构、服务对象、用户规模、业务周期、运行高峰期等；

b） 应掌握业务主管部门、运维机构、系统开发商和集成商、上线运行及系统升级日期等；

c） 应掌握定级情况、数据集中情况、灾备情况等。

7.3.3.2 系统构成情况梳理

评估方应检查被评估方信息系统相关的软硬件构成情况，了解掌握软硬件资产信息并记录结果，包括：

a） 应重点梳理主要硬件设备类型、数量、生产商情况，硬件设备类型主要有：服务器、终端计算机、路由器、交换机、存储设备、防火墙、终端计算机、磁盘阵列、磁带库及其他主要安全设备；

b） 应重点梳理主要软件类型、套数、生产商情况，软件类型主要有：操作系统、数据库管理软件、公文处理软件、邮件系统及主要应用系统。

7.3.4 网络安全应急管理

评估方应检查被评估方网络安全应急管理情况，并检查下列内容：

a） 应制定网络安全事件应急预案，原则上每年评估一次，并根据实际情况适时修订；

b） 应组织开展应急预案的宣贯培训，确保相关人员熟悉应急预案；

c） 应每年开展网络安全应急演练，检验应急预案的可操作性，并将演练情况报网络安全主管部门；

d） 应建立网络安全事件报告和通报机制，提高预防预警能力；

e） 应明确应急技术支援队伍，做好应急技术支援准备；

f） 应做好网络安全应急物资保障，确保必要的备机、备件等资源到位；

g） 应根据业务实际需要对重要数据和业务系统进行备份。

7.3.5 网络安全教育培训

评估方应检查被评估方网络安全教育培训情况，并检查下列内容：

a） 应定期开展网络安全宣传和教育培训工作，提高网络安全意识，增强网络安全基本防护技能；

b） 应定期开展网络安全管理人员和技术人员专业技能培训，提高网络安全工作能力和水平；

c） 应记录并保存网络安全教育培训、考核情况和结果。

7.3.6 外包服务管理

评估方应检查被评估方外包服务管理情况，并检查下列内容：

a） 应建立并严格执行信息技术外包服务安全管理制度；

b） 应与信息技术外包服务提供商签订服务合同和网络安全与保密协议，明确网络安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何资产，不得以服务为由强制要求委托方购买、使用指定产品；

c） 信息技术现场服务过程中应安排专人陪同，并详细记录服务过程；

d） 外包开发的系统、软件上线应用前应进行安全测评，要求开发方及时提供系统测试用例及测试结果、软件的升级、漏洞等信息和相应服务；

e） 外包开发的系统、系统发生版本迭代更新时，应要求开发方提供系统版本迭代说明，说明内容包含但不限于系统功能，影响范围等相应内容；

f） 信息系统运维外包不得采用远程在线运维服务方式。

7.3.7 应用系统安全防护（基本情况）

评估方应检查被评估方应用系统安全防护情况，并检查下列内容：

a） 应按照GB/T 20984-2007的要求，定期对信息系统面临的安全风险和威胁、薄弱环节以及防护措施的有效性等及进行分析评估；

b） 应综合考虑信息系统的重要性、涉密程度和面临的网络安全风险等因素，按照国家网络安全等级保护相关政策和技术标准规范，对信息系统实施相应等级的安全管理；

c） 应按照GB/T 22240-2020的要求，确定信息系统安全保护等级；
d） 应按照GB/T 22239-2019的要求，对信息系统实施相应等级的安全建设和整改；
e） 应按照信息系统安全等级保护测评相关要求，对信息系统进行等级测评。

7.3.8 网络安全自评估

评估方应检查被评估方网络安全自评估情况，并检查下列内容：
a） 应参照本文件中的流程、程序及内容，认真组织开展网络安全自评估工作，掌握网络安全总体状况和面临的威胁，查找安全隐患，堵塞安全漏洞，完善安全措施，减少安全风险，提高安全防护能力；
b） 应每年至少进行一次网络安全自评估，具体时间和范围应根据系统的上线时间、系统的变更情况、事件的发生频率、威胁的严重程度等因素确定；
c） 应加强自评估工作组织领导，建立评估工作责任制，制定评估工作方案并认真落实；
d） 应重视安全技术检测，采取必要的技术检测手段对信息系统、服务器、终端计算机等进行安全检测，可根据需要委托符合要求的检测机构进行技术检测；
e） 应加强安全评估过程中的保密管理和风险控制，严格检查人员、有关文档和数据的安全保密管理，制定安全评估应急预案，确保被评估信息系统的正常运行；
f） 应对评估中发现的问题进行分析研判，制定整改措施并及时整改；
g） 应对年度安全评估情况进行全面总结，按照要求如实完成评估报告并报网络安全主管部门。

7.3.9 网络安全风险规避

评估方应检查被评估方是否采取了网络安全风险规避措施，降低网络安全事件发生时产生的影响和损失，并检查下列内容：
a） 应对安全投入及安全管控的持续性和有效性进行评估；
b） 应制定明确的风险转嫁策略机制；
c） 应根据评估结果采取损失补偿机制和风险防范机制。

7.4 安全技术措施评估

7.4.1 基本要求

评估方应检查被评估方安全技术措施基本情况，并检查下列内容：
a） 开展信息化建设与网络安全建设应按照同步规划、同步建设、同步运行的原则，建立健全的网络安全防护体系；
b） 应根据信息化发展情况通过科学的方式制定了清晰的网络安全建设发展规划路线；
c） 应基于业务链的关联关系进行网络安全风险分析；
d） 应结合现有业务场景的变化、新兴技术的变化采取针对性的防护策略；
e） 应随着业务的变化动态设置或调整网络安全防护体系框架。

7.4.2 物理环境安全防护

评估方应检查被评估方物理环境安全防护情况，并检查下列内容：
a） 机房应采取防盗窃、防破坏、防雷击、防火、防水、防潮、防静电等安全措施；
b） 机房应配备备用电源，采取温湿度控制、电磁防护等安全防护措施；
c） 机房应采取物理访问控制措施，配备门禁系统或有专人值守。

7.4.3 关键设备安全防护

评估方应检查被评估方关键设备安全防护情况，并检查下列内容：

a） 应定期对恶意代码防护设备（如防病毒网关）的恶意代码库进行更新；

b） 服务器（应用系统服务器、数据库服务器）应配置口令策略，包括口令强度和更新频率；应配置安全审计策略，包括启用审计功能、留存操作记录、定期分析日志、对异常访问和操作及时进行处置；应配置病毒防护策略，包括安装防病毒软件、及时更新病毒库；应及时更新补丁，包括操作系统、数据库管理系统等的补丁；

c） 网络设备、安全设备，应配置口令策略，包括口令强度和更新频率；应配置安全审计策略，包括启用审计功能、留存操作记录、定期分析日志、对异常访问和操作及时进行处置。

7.4.4 应用系统安全防护（门户网站）

评估方应检查被评估方应用系统安全防护情况，并检查下列内容：

a） 网站开通前，应组织专业技术机构进行安全测评，对新增应用要进行安全评估；

b） 应定期对网站链接进行安全性和有效性检查；

c） 应采取必要的技术措施，提高网站防篡改、防攻击能力，加强网站敏感信息保护；

d） 应建立完善网络信息发布审核制度，明确审核程序，严格审核流程。

7.4.5 重要数据安全防护

评估方应检查被评估方重要数据安全防护情况，并检查下列内容：

a） 应采用技术措施（如加密、分区分域存储等）对存储的重要数据进行保护；

b） 应采取技术措施对传输的重要数据进行加密和校验；

c） 对于接口类应用程序，应采用校验技术或密码技术保证重要数据在传输过程中的完整性和保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息。

7.4.6 停止安全服务应对处置

评估方应检查被评估方停止安全服务应对处置情况，并检查下列内容：

a） 应对仍在使用的停止安全服务的操作系统、数据库软件、中间件、应用系统的计算机进行归类，并将其纳入重点防护范围；

b） 应针对操作系统、数据库软件、中间件、应用系统停止服务不能进行安全补丁更新的计算机制定专门的安全保护方案，建立漏洞核查机制，持续监测漏洞的通报情况，并利用微隔离、入侵防御、安全加固等技术手段加强计算机威胁传播、攻击和破坏的防御能力；

c） 应卸载仍使用停止安全服务的操作系统、数据库软件、中间件、应用系统计算机中与工作无关的应用程序，只允许安装及运行管理员确认过的软件；应禁用、限制使用USB设备；应关闭不必要的服务和端口。

7.4.7 数据泄露及系统被控防护

评估方应检查被评估方数据泄露及系统被控防护情况，并检查下列内容：

a） 数据中心的设备机房应位于中国境内；

b） 采用第三方的云计算服务，应记录云计算服务商情况；

c） 外包服务商提供服务过程中应有专人陪同，应禁止远程在线维护。

7.4.8 网络边界安全防护

评估方应检查被评估方网络边界安全防护情况，并检查下列内容：

a） 非涉密信息系统与互联网及其他公共信息网络应实行逻辑隔离，涉密信息系统与互联网及其他公共信息网络应实行物理隔离；

b） 建立互联网接入审批和登记制度，严格控制互联网接入口数量，加强互联网接入口安全管理和安全防护；

c） 应采取访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范等措施，进行网络边界防护；

d） 应根据承载业务的重要性对网络进行分区分域管理，采取必要的技术措施对不同网络分区进行防护、对不同安全域之间实施访问控制；

e） 应对网络日志进行管理，定期分析，及时发现安全风险。

7.4.9 无线网络安全防护

评估方应检查被评估方无线网络安全防护情况，并检查下列内容：

a） 应采取身份鉴别、地址过滤等措施对无线网络的接入进行管理，采取白名单管理机制，防止非授权接入造成的内网渗透事件发生；

b） 应采用与有线边界相同的安全防护手段，对常见的无线攻击进行防御；

c） 应修改无线路由设备的默认管理地址；

d） 应修改无线路由管理账户默认口令，设置复杂口令，防止暴力破解后台；

e） 用户接入认证加密应采用WPA2及更高级别算法，防止破解接入口令。

7.4.10 电子邮件系统安全防护

评估方应检查被评估方电子邮件系统安全防护情况，并检查下列内容：

a） 应加强邮件系统安全防护，采取反垃圾邮件等技术措施；

b） 应规范电子邮箱的注册管理，原则上只限于本部门工作人员注册使用；

c） 应严格管理邮箱账号及口令，采取技术和管理措施确保口令具有一定强度并定期更换。

7.4.11 终端计算机安全防护

评估方应检查被评估方终端计算机安全防护情况，并检查下列内容：

a） 应采取集中统一管理方式对终端计算机进行管理，统一软件下发，统一安装系统补丁，统一实施病毒库升级和病毒查杀，统一进行漏洞扫描；

b） 应规范软硬件使用，不得擅自更改软硬件配置，不得擅自安装软件；

c） 应加强账户及口令管理，使用具有一定强度的口令并定期更换；

d） 应对接入重要的终端计算机采取控制措施，包括双因素认证、实名接入认证、IP地址与MAC地址绑定等；

e） 应定期对终端计算机进行安全审计；

f） 非涉密计算机不得存储和处理国家秘密信息。

7.4.12 存储介质防护

评估方应检查被评估方存储介质防护情况，并检查下列内容：

a） 应严格存储阵列、磁带库等大容量存储介质的管理，采取技术措施防范外联风险，明确存储数据安全；

b） 应对移动存储介质进行集中统一管理，记录介质领用、交回、维修、报废、销毁等情况；

c） 非涉密移动存储介质不得存储涉及国家秘密的信息，应在涉密计算机上使用；
d） 移动存储介质在接入本部门计算机和信息系统前，应查杀病毒、木马等恶意代码；
e） 应配备必要的电子信息消除和销毁设备，对变更用途的存储介质要消除信息，对废弃的存储介质要进行销毁。

7.4.13 漏洞修复

评估方应检查被评估方漏洞修复情况，并检查下列内容：
a） 应定期对本单位主机、网络安全防护设备、信息系统进行漏洞检测，对于发现的安全漏洞及时进行修复处置；
b） 重视自行监测发现与第三方漏洞通报机构告知的漏洞风险，及时处置。

7.5 技术检测评估

评估方应利用技术手段对被评估可能存在的脆弱性进行针对性的检测，主要包括：
a） 应重点对认定为关键信息基础设施的信息系统进行安全检测；
b） 应使用漏洞扫描等工具测试关键信息基础设施是否存在安全漏洞；
c） 应开展人工渗透测试，检查是否可以获取应用系统权限，验证网站是否可以被挂马、重改页面、获取敏感信息等，检查系统是否被入侵过（存在入侵痕迹）等；
d） 应根据工作实际合理安排年度检测的服务器数量，每1年～2年对所有服务器进行一次技术检测，重要业务系统和门户网站系统的服务器应作为检测重点；
e） 应使用病毒木马检测工具，检测服务器是否感染了病毒、木马等恶意代码；
f） 应使用漏洞扫描等工具检测服务器操作系统、数据库、应用、端口、服务及补丁更新情况，检测是否关闭了不必要的端口、应用、服务，是否存在安全漏洞。

附 录 A
（资料性）
记录表

信息系统基本信息记录表见表A.1。

表 A.1 信息系统基本信息记录表

系统名称	
主要业务	
操作对象	
与危险源关联情况	
部署位置	
网络拓扑结构	
连接互联网情况	
操作系统名称型号	
系统所在网段	
数据集中情况	
数据灾备情况	
服务对象	
用户规模	
业务周期	
业务主管部门	
运维机构	
系统开发商	
系统集成商	
上线运行及最近一次系统升级时间	
系统定级情况	

信息系统资产记录表见表A.2。

表 A.2 资产记录表

编号	资产名称	品牌和型号	数量	IP 地址	物理位置	业务应用	是否为关键资产
1							
2							
3							
4							
5							
6							

附 录 B
（资料性）
风险分析模型

对风险进行计算，需要确定影响风险要素、要素之间的组合方式以及具体的计算方法，将风险要素按照组合方式使用具体的计算方法进行计算，得到风险值。目前通用的风险评估中风险值计算涉及的风险要素一般为资产、威胁、和脆弱性；这些要素的组合方式如图A.1风险计算原理中指出，由威胁和脆弱性确定安全事件发生可能性，由资产和脆弱性确定安全事件的损失，以及由安全事件发生的可能性和安全事件的损失确定风险值。

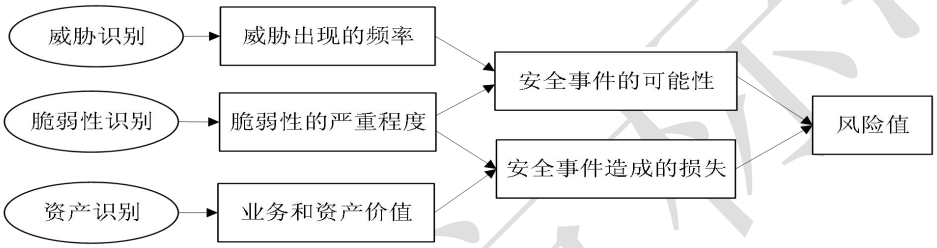

图 B.1 风险计算原理

使用相乘法计算风险（也可采用矩阵法），风险值=$\sqrt{T*V}*\sqrt{A*V}$，A（1～5）为资产值，T（1～5）为威胁值，V（1～5）为脆弱性值。

按照上述方法进行计算，得到资产的风险值。为实现对风险的控制与管理，可以对风险评估的结果进行等级化处理。等级化处理的方法是按照风险值的高低进行等级划分，风险值越高，风险等级越高。风险等级一般可划分为五级。

确定风险等级划分如表 A.1 所示。

表 B.1 风险等级划分表

风险值	1-5	6-10	11-15	16-20	21-25
风险等级	1	2	3	4	5

根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。表A.2提供了一种风险等级划分方法。

表 B.2 风险等级描述表

等级	标识	描述
5	很高	一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重影响组织的正常经营，经济损失重大、社会影响恶劣
4	高	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补

附 录 C
（资料性）
评估报告模板示例

以下为网络安全评估报告模板示例，仅供参考。

网络安全评估报告格式

项 目 名 称： _____

项目建设单位： _____

风险评估单位： _____

年 月 日

目　　录

一、风险评估项目概述

1.1 工程项目概况

1.1.1 建设项目基本信息

工程项目名称		
工程项目批复的建设内容	非涉密信息系统部分的建设内容	
	相应的信息安全保护系统建设内容	
项目完成时间		
项目试运行时间		

1.1.2 建设单位基本信息

工程建设牵头部门

部门名称	
工程责任人	
通信地址	
联系电话	
电子邮件	

工程建设参与部门

部门名称	
工程责任人	
通信地址	
联系电话	
电子邮件	

如有多个参与部门，分别填写上

1

1.1.3 承建单位基本信息

如有多个承建单位，分别填写下表。

企业名称	
企业性质	是国内企业/还是国外企业
法人代表	
通信地址	
联系电话	
电子邮件	

1.2 风险评估实施单位基本情况

评估单位名称	
法人代表	
通信地址	
联系电话	
电子邮件	

二、风险评估活动概述

2.1 风险评估工作组织管理

描述本次风险评估工作的组织体系（含评估人员构成）、工作原则和采取的保密措施。

2.2 风险评估工作过程

工作阶段及具体工作内容.

2.3 依据的技术标准及相关法规文件

2.4 保障与限制条件

需要被评估单位提供的文档、工作条件和配合人员等必要条件，以及可能的限制条件。

三、评估对象

3.1 评估对象构成与定级

3.1.1 网络结构

文字描述网络构成情况、分区情况、主要功能等，提供网络拓扑图。

3.1.2 业务应用

文字描述评估对象所承载的业务，及其重要性。

3.1.3 子系统构成及定级

描述各子系统构成。根据安全等级保护定级备案结果，填写各子系统的安全保护等级定级情况表：

各子系统的定级情况表

序号	子系统名称	安全保护等级	其中业务信息安全等级	其中系统服务安全等级

3.2 评估对象等级保护措施

按照工程项目安全域划分和保护等级的定级情况，分别描述不同保护等级保护范围内的子系统各自所采取的安全保护措施，以及等级保护的测评结果。

根据需要，以下子目录按照子系统重复。

3.2.1 XX 子系统的等级保护措施

3.2.2 子系统 N 的等级保护措施

四、资产识别与分析

4.1 资产类型与赋值

4.1.1 资产类型

按照评估对象的构成，分类描述评估对象的资产构成。详细的资产分类与赋值，以附件形式附在评估报告后面。

4.1.2 资产赋值

填写《资产赋值表》。

资产赋值表

序号	资产编号	资产名称	子系统	资产重要性

4.2 关键资产说明

在分析被评估系统的资产基础上，列出对评估单位十分重要的资产，作为风险评估的重点对象，并以清单形式列出如下：

关键资产列表

资产编号	子系统名称	应用	资产重要程度权重	其他说明

五、威胁识别与分析

对威胁来源（内部/外部；主观/不可抗力等）、威胁方式、发生的可能性，威胁主体的能力水平等进行列表分析。

5.1 威胁数据采集

5.2 威胁描述与分析

依据《威胁赋值表》，对资产进行威胁源和威胁行为分析。

5.2.1 威胁源分析

填写《威胁源分析表》。

5.2.2 威胁行为分析

填写《威胁行为分析表》。

5.2.3 威胁能量分析

5.3 威胁赋值

填写《威胁赋值表》。

六、脆弱性识别与分析

按照**检测对象**、**检测结果**、**脆弱性分析**分别描述以下各方面的脆弱性检测结果和结果分析。

6.1 常规脆弱性描述

6.1.1 法律法规合规脆弱性

6.1.2 行业领域要求脆弱性

6.1.3 安全管理措施脆弱性

6.1.4 安全技术措施脆弱性

6.2 脆弱性专项检测

6.2.1 渗透测试专项测试

6.2.2 恶意代码专项检查

6.2.3 安全漏洞专项测试

6.3 脆弱性综合列表

填写《脆弱性分析赋值表》。

七、风险分析

7.1 关键资产的风险计算结果

填写《风险列表》

风险列表

资产编号	资产风险值	资产名称

7.2 关键资产的风险等级

7.2.1 风险等级列表

填写《风险等级表》

资产风险等级表

资产编号	资产风险值	资产名称	资产风险等级

7.2.2 风险等级统计

资产风险等级统计表

风险等级	资产数量	所占比例

7.2.3 基于脆弱性的风险排名

基于脆弱性的风险排名表

脆弱性	风险值	所占比例

7.2.4 风险结果分析

八、综合分析与评价

九、整改意见

参 考 文 献

[1] GB/T 29245-2012 信息安全技术 政府部门信息安全管理指南
[2] GB/T 36466-2018 信息安全技术 工业控制系统风险评估实施指南
[3] 《中华人民共和国网络安全法》，2016
[4] 《关于开展关键信息基础设施网络安全检查的通知》，中网办发[2016]3号
[5] 《网络安全审查办法》，2020