ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

T/

中 国 网 络 安 全 产 业 联 盟 团 体 标 准

T/XXX XXXX—XXXX

网络安全保险 安全风险评估实施指南

Cyber Security Insurance Guide of implementation for security risk assessment

（征求意见稿）

（本征求意见稿完成时间：2021 年 12 月）

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

中国网络安全产业联盟 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。

本文件由中国网络安全产业联盟提出。

本文件由中国网络安全产业联盟归口。

本文件起草单位：杭州安恒信息技术股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、亚信科技（成都）有限公司、北京启明星辰信息安全技术有限公司、北京梆梆安全科技有限公司、上海观安信息技术股份有限公司、北京瑞和云图科技有限公司、北京六方云信息技术有限公司、上海竟安网络科技有限公司、网宿科技股份有限公司、光通天下网络科技股份有限公司、国网思极网安科技（北京）有限公司、北京元支点信息安全技术有限公司、北京华圣龙源科技有限公司

本文件主要起草人：

引　　言

网络安全保险作为风险转移的重要手段，得到越来越多的关注。现阶段开展网络安全保险业务时，对潜在投保用户的信息系统进行网络安全风险评估存在不足，缺乏规范的评估过程、指标和方法指引，极大影响网络安全保险在国内的推广和应用。本文件试图通过建立一套风险评估指标、流程、内容，规范对拟投保系统的风险评估，得出风险等级、风险分值，定量化的呈现拟投保系统网络安全风险状况，为后续开展网络安全保险业务提供参考依据。

网络安全保险 安全风险评估实施指南

1 范围

本文件规范了网络安全保险投保阶段的网络安全风险评估实施过程，规范了网络安全保险通用场景和数据安全、网络勒索和业务连续性中断三类典型场景的风险计算方法。

本文件适用于指导网络安全服务提供商在网络安全保险投保阶段开展网络安全风险评估活动。可为保险公司、再保险公司开展网络安全保险业务前的风险评估与风险定价等提供指导，也可为网络安全保险投保人或被保险人开展网络安全风险自评估提供参考。

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。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 31509 信息安全技术 信息安全风险评估实施指南

GB/T 36687-2018 保险术语

3 术语和定义

GB/T 20984、GB/T 31509和GB/T 36687-2018界定的以及下列术语和定义适用于本文件。

3.1

风险 risk

一个给定的威胁，利用一项资产或多项资产的脆弱性，对组织造成损害的潜能。可通过事件的概率及其后果进行度量。

3.2

网络安全风险 cyber security risk

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.3

风险评估 risk assessment

风险标识、分析和评价的整个过程。

3.4

（网络安全）风险评估（cyber security）risk assessment

依据有关网络安全技术与管理标准，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。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

3.5

网络安全事件 cyber security incident

网络安全事件是由单个或一系列意外或有害的网络安全事态所组成的，极有可能危害业务运行或威胁信息安全。

3.6

安全控制 security controls

为保护某一系统及其信息的保密性、完整性和可用性以及可核查性、真实性、抗抵赖性、私有性和可靠性等，而对信息系统所选择并施加的管理、操作和技术等方面的控制(即防御或对抗)。

3.7

资产 asset

对组织具有价值的任何东西。

3.8

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

3.9

脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

3.10

评估要素 assessment factor

风险评估活动中必须要识别、分析的一系列基本因素。

3.11

网络安全保险 cybersecurity insurance

网络安全保险是以投保人信息资产安全性（信息的完整性、机密性、有效性等）为保险标的的保险服务产品。对由于网络安全事件给组织造成的负面影响进行赔偿，赔偿内容包括组织本身财产损失也包含第三方赔偿责任。

3.12

投保人 applicant;proposer

与保险人订立保险合同，并按照保险合同负有支付保险费义务的人。

3.13

被保险人 insured

其财产或者人身受保险合同保障,享有保险金请求权的人。

注：投保人可以为被保险人

3.14

保险人 insurer

又称“承保人”，是指与投保人订立保险合同，并承担赔偿或者给付保险金责任的保险公司。

3.15

再保险人 reinsurer

再保险人是指接受原保险人分出的再保险业务，对再保险合同的原保险人所发生的保险赔付承担赔偿责任的主体，也叫再保险接受人或分入人、分入公司。

3.16

风险单位（Unit of exposure）

风险单位在保险中是指保险标的发生一次灾害事故可能造成的最大损失范围。风险单位的划分标准既重要又复杂，应根据不同的标的和险种来决定。

4 网络安全保险安全风险评估概述

4.1 实施原则

4.1.1 最小影响

对于信息系统的风险评估，应采用最小影响原则，即首要保障信息系统的稳定运行，而对于需要进行攻击性测试的工作内容，需与用户沟通并进行应急备份，同时选择避开业务的高峰时间运行。

4.1.2 客观诚信

开展网络安全保险安全风险评估工作应建立在双方（投保人和评估方）诚信的基础之上，投保人在访谈过程中应如实陈述或承诺自身的网络安全情况，评估方在评估过程中应客观公正的记录和分析投保人的网络安全情况。

4.1.3 数据保护

对在风险评估过程中所接触到的业务数据、系统数据及其他相关数据进行安全保护,包括但不限于：人员操作行为审计、数据安全意识培训等，防止数据以任何形式被泄露、窃取和篡改，确保数据安全。

4.1.4 量化评估

针对网络安全保险业务的安全风险评估应最大程度地确保评估结果能够量化，以便于后续保险业务的开展。

4.1.5 范围完整

网络安全保险安全风险评估应以被评估组织的风险单元作为评估工作的核心，把涉及风险单元相关的业务、系统、网络、数据、应用平台等作为评估工作的重点范围，全面评估风险单元的网络安全风险。

4.1.6 边界明确

网络安全保险安全风险评估时应划分风险单位，根据投保人的业务类型、系统重要性、影响程度等来明确评估单元。

4.2 实施方法

开展网络安全保险安全风险评估工作所采用的评估方法，主要包括访谈、检查和测试3种。

访谈由评估人员与风险单元相关的管理人员、操作人员、服务人员等进行谈话，以促进对保险标的物安全控制措施实施情况的了解、分析或证据获取。访谈的对象为个人或团体。

注：访谈对象可以是组织高管、CIO、信息安全机构领导、信息系统安全管理员、运维人员、网络和系统管理员、机房安全管理人员和用户等。

检查由评估人员通过对管理制度、安全策略和机制、安全配置和设计文档、运行记录等进行观察、查验、分析以帮助评估人员理解、分析或取得证据的过程。检查的对象为规范、机制和活动。

注：检查活动可以是评审信息安全策略规划和程序、分析系统的设计文档和接口规范、观测系统的备份操作、审查应急演练结果、观察事件响应活动、研究技术手册和用户 / 管理员指南及检查信息系统安全基线配置等。

测试由评估人员进行技术测试，通过人工或自动化安全测试工具获得相关信息，并进行分析以帮助评估人员获取证据的过程。测试的对象为机制和活动。

注：测试方式可以是渗透测试、安全机制测试、安全基线核查、数据备份与恢复测试、事件响应能力以及应急规划演练能力测试等。

4.3 险别分类

常见的网络安全保险险别分类见表1，其中，不同险别在脆弱性识别时会存在额外的拓展项，参见本文件第8章的内容。

表1 常见的网络安全保险险别分类

序号	大类	险别	描述
1	第一方损失	应急服务+数据恢复费用	对被保险人因与下述事项有关所发生的合理费用和支出承担相应的赔偿责任： (i)确定电子数据是否能够恢复、重建或重新收集；以及 (ii)如有可能，恢复、重建或重新收集电子数据。
2		网络勒索威胁和勒索支付款项	保险人负责向被保险人进行补偿，被保险人实际支付的因网络勒索威胁直接引起的勒索费用和勒索支付款项。

表1 常见的网络安全保险险别分类（续）

序号	大类	险别	描述
3		营业收入损失和从属营业收入损失	被保险人因服务中断在恢复期限内发生的营业收入损失、从属营业收入损失和额外费用，保险人向被保险人进行补偿。

序号	大类	险别	描述
4	第三者责任	外包商数据安全责任	被保险企业的信息外包服务商因遭遇未经授权访问导致信息泄露，被保险人被数据泄露信息主体起诉而产生的法定赔偿责任
5		数据安全责任	被保险企业信息系统遭受未经授权访，导致客户信息泄露，被保险人被信息泄露主体起诉而产生的法定赔偿责任

注：保险相关描述最终以各保险公司条款为准。

4.4 投保流程

4.4.1 相关参与方

网络安全保险投保阶段的风险评估过程一般涉及四个相关方，包括：

a) 投保人/被保险人：投保人指与保险人订立保险合同，并按照保险合同约定负有支付保费义务。被保险人受保险合同保障,享有保险金请求权的人。投保人与被保险人可以为同一人。在网络安全保险语境中，投保人和被保险人指有潜在投保意愿，网络安全能力达到一定水平的组织；
b) 保险人：提供网络安全保险业务的保险公司；
c) 再保险人：提供网络安全保险业务再保支持的公司；
d) 网络安全服务提供商：为网络安全保险提供风险评估、技术支持等安全服务的公司。

4.4.2 投保流程

网络安全保险投保流程见图1，本文件在投保阶段流程中的应用环节是指导和规范网络安全风险评估方提供网络安全保险安全风险评估工作的实施。

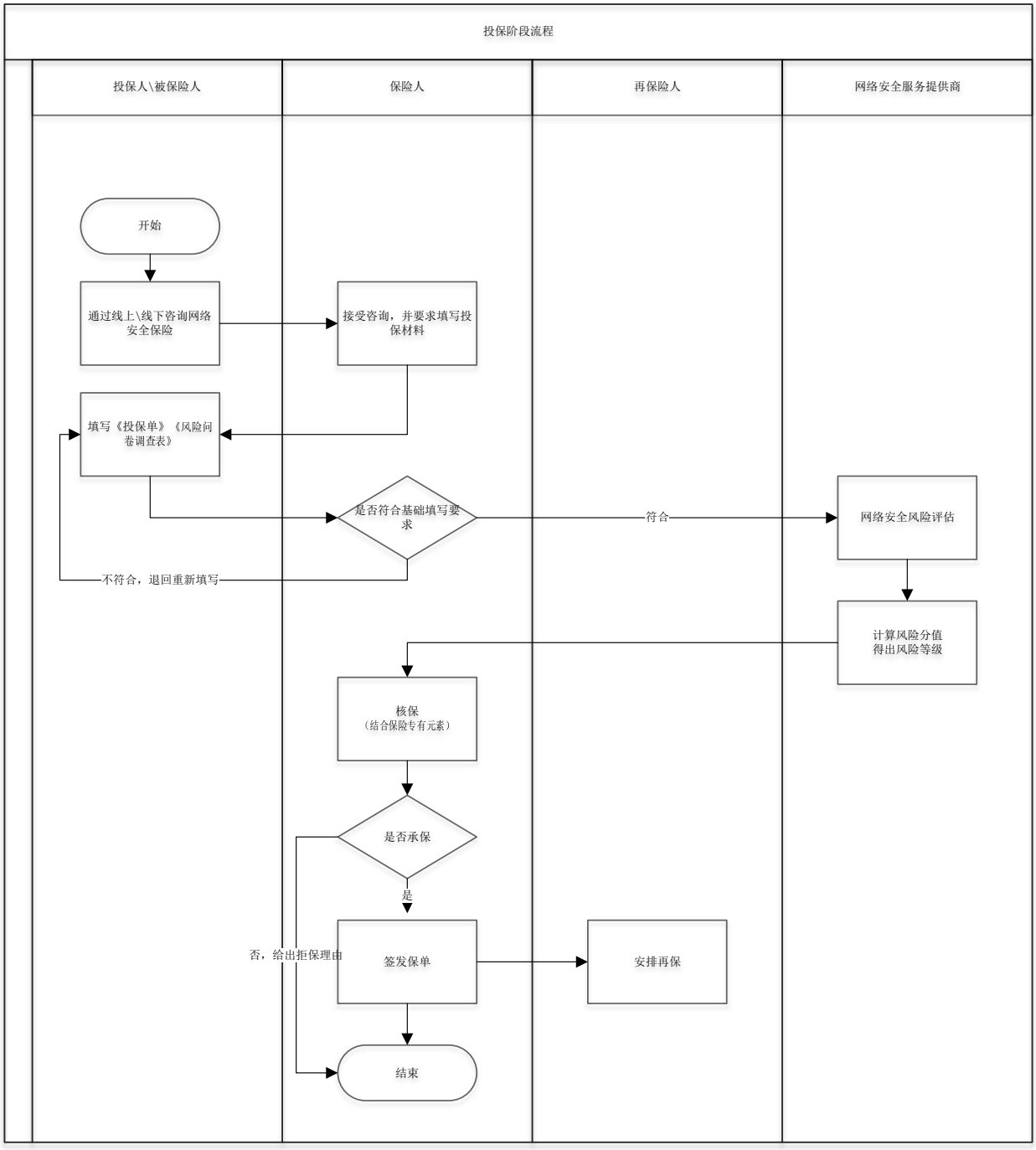


图1　网络安全保险投保流程

5　网络安全保险安全风险评估实施流程

在网络安全保险网络安全风险评估活动中，一般流程按照GB/T 20984-2007规定的评估准备阶段、风险要素识别阶段、风险分析与计算阶段、保险人核保阶段四个阶段进行。如图2所示：

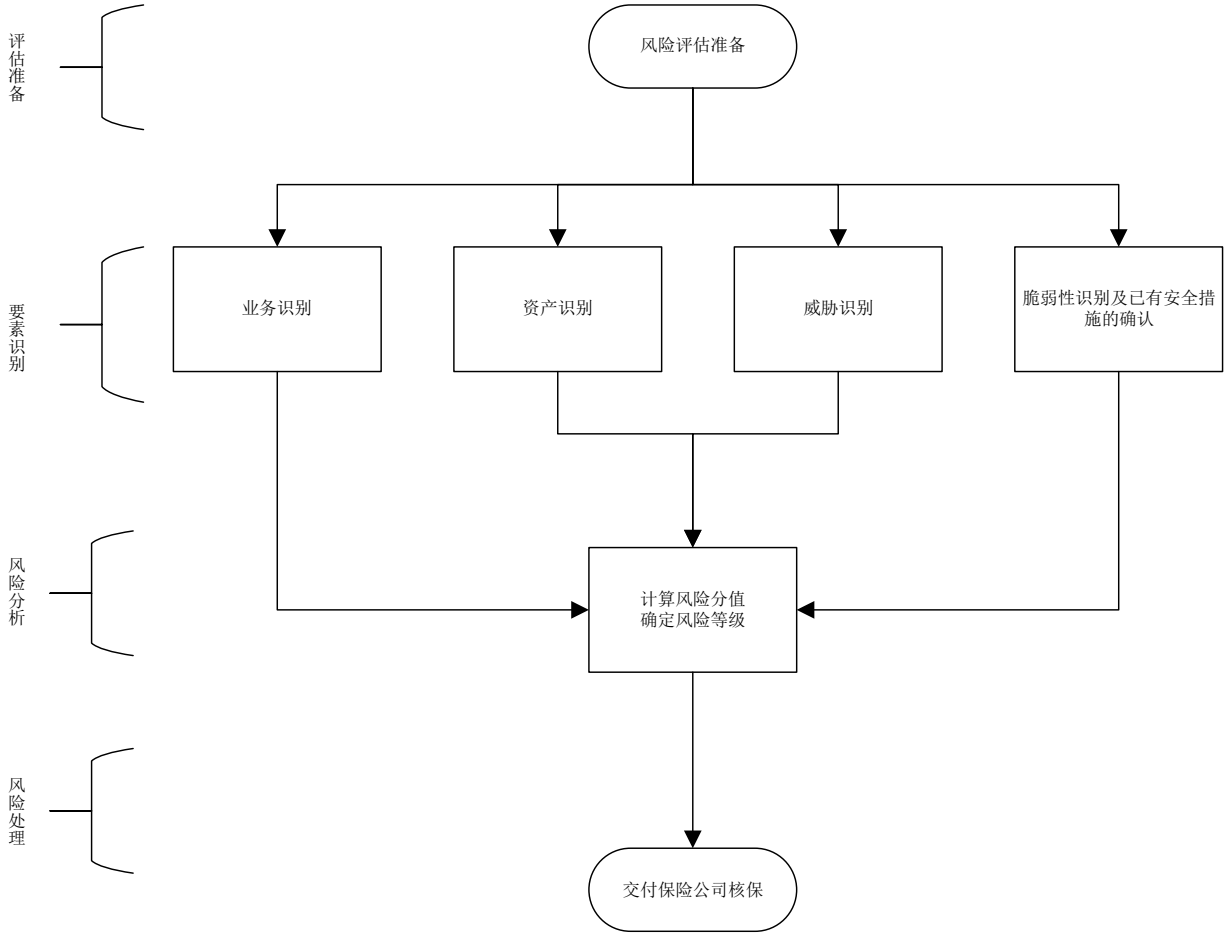


图2　网络安全保险风险评估流程

5.1　评估准备阶段

保险人、再保险人在开展网络安全保险业务时，通常涉及一些准备活动，此类活动主要包括：

a)　向被评估方发送评估通知，告知评估相关内容

b)　与被评估方协调评估获取拟投保人已经实施的网络安全控制措施；

c)　评估被保险人的网络安全风险；

d)　评估被保险人的经营风险；

5.2　风险评估要素识别阶段

在网络安全保险风险评估活动中，应识别的风险要素有业务、资产、威胁和脆弱性（含已有安全控制措施），具体如下：

a)　业务识别。业务识别分为三个步骤：第一步是业务板块识别、承载业务板块功能的信息系统的识别，即识别组织拟投保的业务板块有哪些，以及承载业务的信息系统有哪些；第二步是风险单位的划分；第三步是根据重要性分别对业务板块、信息系统赋予权重，并得到被评估方的认可。具体步骤见 6.1；

b)　资产识别。资产识别分三个步骤：第一步识别出各信息系统承载的资产数量、类型等；第二步根据资产重要性赋予不同的系数值。资产保密性、完整性和可用性是评价资产的三个安全属性，结合拟投保标的物在保险维度的价值，综合上述维度将资产区分为 5 个级别（第 5 级最高）；第三步赋予权重，根据信息系统下承载的资产重要性分别赋值，并得到被评估方的认可。具体步骤见 6.2；

c) 威胁识别。动机、能力和频率是威胁的属性，据此将威胁能力赋值划分为 5 个级别（第 5 级最高），判断依据应在评估准备阶段根据历史统计或行业判断予以确定，并得到被评估方的认可。具体步骤见 6.3；
d) 脆弱性识别（含已有安全控制措施）。分成风险类型、识别类、识别项、识别内容四大类。根据网络安全高低分为 5 个级别（第 5 级最高），每一个级别对应区间分数值。在做脆弱性识别时应同时识别出已有安全控制措施，具体步骤见 6.4。

5.3 风险分析与计算阶段

网络安全保险网络风险评估根据业务、资产、威胁、脆弱性（含已有安全控制措施）的估算评分，计算得出风险分值、风险等级。具体如下：

a) 业务打分。具体步骤见 7.1；
b) 资产打分。具体步骤见 7.2；
c) 威胁打分。具体步骤见 7.3；
d) 脆弱性打分（含已有控制措施）。具体步骤见 7.4；
e) 计算综合风险分值、风险等级。具体步骤见 7.5。

5.4 保险人核保阶段

参与方按照本文件，计算得出保险标的物的风险等级、风险分值等量化指标后交付保险人。保险人再结合保险属性（如评估被保险人的行业属性、商业风险、法律风险、历史风险发生情况等），决定是否承保，并提供保险报价。

6 网络安全保险风险要素识别

6.1 业务识别

业务识别时的数据可来自于熟悉组织业务结构的业务人员或管理人员。业务识别即可通过访谈、文档查阅、资料查阅，还可通过对信息系统进行梳理后总结整理进行补充。

业务识别需要识别出组织拟投保的业务板块，承载各业务的信息系统数量、类型；并对业务板块、信息系统做风险单位划分；对业务板块、信息系统的重要性赋予不同的权重。业务识别时应针对业务流程，识别业务与信息系统、平台或支撑系统的逻辑关联性，识别用于支撑业务活动的基础设施、信息资产和资源。

6.1.1 业务板块识别

业务板块识别时可以参考：业务的定位、业务关联性、业务完整性、业务流程。如表2所示。

表2 业务板块识别内容

分类	示例
定位	业务：业务功能、业务对象、业务范围。 战略地位：发展战略中的业务属性和职能定位、与发展战略目标的契合度、业务布局中的位置和作用、竞争关系中竞争力强弱等
业务关联性	并列关系：业务与业务间并列关系包括业务间相互依赖或单向以来，业务间共用同一信息系统，业务属于同一业务流程的不同业务环节等 父子关系：业务与业务之间存在包含关系等 间接关系：通过其他业务，或者其他业务流程产生的关联性等
业务完整性	独立业务：业务独立，整个业务流程和环节闭环 非独立业务：业务属于业务环节的某一部分。可能与其他业务具有关联性。

表2　业务板块识别内容（续）

分类	示例
业务流程	业务逻辑：业务的输入、输出、执行过程中逻辑的完整性、可用性、合理性与安全性，通过询问、查看或使用测试用例进行测试的方法进行业务流程识别，判断流程中所涉及的业务逻辑是否得到完整、合理和安全的执行。 数据流：数据在业务流程中的流转、在系统内部或不同系统之间的输入与输出、相关接口等。 流程管理审批：流程步骤、审评控制和人员等。业务流程分析关注业务数据流和业务控制流，既关注数据的流转安全，也关注数据流的关键控制点。

6.1.2　信息系统识别

识别出某一业务板块下承载的信息系统数量、类型等基本信息。

6.1.3　风险单位划分

风险单位划分在保险中是指识别保险标的发生一次灾害事故可能造成的最大损失范围。本文件所指风险单位除保留保险领域定义之外，也为后续的资产识别、威胁识别、脆弱性识别（含已有安全控制措施识别）后，作为一个基础单元计算风险分值。如表3所示：

表3　风险单位识别内容

投保企业数量	业务板块数量	承载业务的信息系统数量	风险单位识别方法
1	1	1	宜将该信息系统及其资产作为一个风险单位，进行识别；
1	1	N	宜将该业务板块承载的所有信息系统及其资产作为一个风险单位，进行识别；
1	N	1	宜将该信息系统及其资产作为一个风险单位，进行识别；
1	N	M	宜将某业务板块承载的所有信息系统及其资产作为一个风险单位进行识别；无论业务板块之间是否存在共同承载的信息系统。

6.1.4　赋予权重

在进行业务板块识别时，可以根据各业务板块的重要性，分别对其设置不同权重（与被评估方沟通，并得到认可），为后续计算风险分值时提供参照依据；对于某一业务板块下承载的各个信息系统，可以根据各信息系统的重要性，分别对其设置不同权重（与被评估方沟通，并得到认可），为后续计算风险分值时提供参照依据。

6.2　资产识别

资产识别主要有两个方面的内容：一是识别出各信息系统承载的资产数量、类型等；二是根据资产重要性赋予不同的系数值。

6.2.1　资产识别

资产识别包括根据资产类别进行识别、资产业务承载性识别和资产关联性识别三个方面。根据资产的表现形式，可将资产分为数据、服务、信息系统、平台或支撑系统、基础设施、人员管理等。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估方灵活把握。表4列出了一种资产分类方法。

表4　基于表现形式的资产分类方法

类别	分类	示例
有形资产	数据	业务生产数据：数据库数据、分布式存储系统数据等 配置、审计、监测数据：系统运行监测数据、运行日志、软硬件配置数据等 文档数据：系统文档、运行管理规程、计划、报告、用户手册、各类纸质的文档等
	信息系统	系统软件：操作系统、数据库管理系统、语句包、开发系统等 应用系统：业务系统等 应用软件：办公软件、各类工具软件、移动应用软件等 源程序：各种共享源代码、自行或合作开发的各种代码等
	平台或支撑系统	平台：支撑系统运行的基础设施平台，如云计算平台、大数据平台等 虚拟化支撑系统：支撑系统运行的虚拟化系统，如虚拟机管理器和虚拟机等 支撑接口：信息系统依赖的第三方平台接口，如云计算PaaS层服务向其他信息系统提供的服务接口等 传统支撑系统：操作系统、数据库管理系统、中间件、开发系统、语句包等
	基础设施	网络设备：路由器、网关、交换机等 安全设备：防火墙、入侵检测/防护系统、防病毒网关、态势感知系统等 计算机设备：大型机、小型机、服务器、工作站、台式计算机、便携计算机等 存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等 传输线路：光纤、双绞线等 保障设备：UPS、变电设备、空调、保险柜、文件柜、门禁、消防设施等 智能终端：感知节点设备（物联网感知终端）、移动终端等 其他：打印机、复印机、扫描仪、传真机等
无形资产	服务	信息服务：对外依赖该系统开展的各类服务 网络服务：各种网络设备、设施提供的网络连接服务 办公服务：为提高效率而开发的管理信息系统，包括各种内部配置管理、文件流转管理等服务 供应链服务：为了支撑业务、信息系统运行、信息系统安全，第三方供应链以及服务商提供的服务等 平台服务：对外依赖云计算平台、态势感知平台等开展的各类服务，如云主机服务、云存储服务等
	人员管理	运维人员：对基础设施、平台、支撑系统、信息系统或数据进行运维的人员，网络管理员、系统管理员等 业务操作人员：对业务系统进行操作的业务人员或管理员等 安全管理人员：网络安全管理员、网络安全管理领导小组等 外包服务人员：外包运维人员、外包安全服务或其他外包服务人员等
	其它	声誉：组织形象、组织信用 知识产权：版权、专利等 业务关系：客户关系、组织关系、政府关系等

对于提供多种业务的组织，其支持业务持续运行的业务组成形式较多，其资产承载情况较为复杂。将信息系统作为纽带，对资产进行业务承载性识别，为下一步的风险评估打下基础。资产业务承载性识别，可按照GB/T 31509-2015，应确定评估对象中包含哪些信息系统,每个信息系统处理哪些种类业务,每种业务包括哪些具体业务功能,以及相关业务处理的流程。分析并清楚理解各种业务功能和流程,有利于分析系统中的数据流向及其安全保证要求。

资产具有关联性，同一资产可能承载了不同的业务。在云计算平台或大数据平台，计算资源、网络资源和存储资源进行了虚拟化，资产间的关联性和安全性有更多相关性。资产关联性识别确定承载哪些业务，这些业务还涉及哪些其他相关资产，关联资产的所有安全级别。

6.2.2　赋予系数值

根据资产重要性，分别对其设置不同系数值，为后续计算风险分值时提供参照依据。

6.2.3　赋予权重

某一信息系统下承载的所有资产，根据其重要性分别赋予权重值（与被评估方沟通，并得到认可），为后续计算风险分值时提供参照依据。

6.3 威胁识别

6.3.1 威胁分类

威胁是一种客观存在的，可能导致危害系统或组织的不希望事故的潜在起因。造成威胁的因素可分为人为因素和环境因素。环境因素中包括自然界不可抗的因素和其它物理因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。威胁作用形式可以是对信息系统直接或间接的攻击，在机密性、完整性或可用性等方面造成损害；也可能是偶然、或蓄意的事件。在对威胁进行分类前，应考虑威胁的来源，如表5所示。

表5 威胁来源列表

来源		描述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通讯线路等方面的故障，或者依赖的第三方平台或者信息系统等方面的故障。
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益。 外部人员利用信息系统的脆弱性，对网络或系统的保密性、完整性和可用性进行破坏，以获取利益或炫耀能力。
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击。

威胁有多种分类方法，下表根据威胁产生的原因、表现和后果不同进行分类，如表6所示。

表6 威胁分类方法

种类	描述	威胁子类
灾害性破坏	由于不可抗力对信息系统造成物理破坏	地震、战争、火灾、水灾、台风、雷击、坍塌、火灾、恐怖袭击、战争
设备设施故障	由于信息系统自身故障或外围保障设施故障，造成信息系统异常或对信息系统当前运行造成潜在危害	软硬件自身故障、外围保障设施故障、人为破坏、其它设备设施故障
信息内容攻击	利用网络发布、传播危害国家安全、社会稳定和公共利益、企业和个人利益的内容的攻击	发布、传播不良信息
信息破坏	通过网络或其它手段，造成信息系统中的信息被篡改、假冒、泄露、窃取等	信息篡改、信息假冒、信息泄露、信息窃取、信息丢失、其它信息破坏
网络攻击	通过网络或其他手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或者使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害	拒绝服务攻击、后门攻击、漏洞攻击、网络扫描攻击、网络钓鱼、干扰、其它网络攻击
有害程序	插入到信息系统中的一段程序，危害系统中数据、应用程序或操作系统的保密性、完整性和可用性，或影响信息系统的正常运行	计算机病毒、蠕虫、特洛伊木马、僵尸网站、混合攻击程序、网页内嵌恶意代码、其它有害程序

6.3.2 威胁能力识别

不同的威胁源具有不同的攻击能力，攻击者的能力越强，攻击成功的可能性就越大。衡量攻击能力的因素主要包括：施展攻击的知识、技能、经验和必要的资金、人力和技术资源等。

6.3.3 威胁频率识别

判断威胁出现的频率是威胁识别的重要内容，评估方应根据经验和有关的统计数据来进行判断。在评估中，需要综合考虑以下四个方面，以形成在某种评估环境中各种威胁出现的频率：

a） 以往安全事件报告中出现过的威胁及其频率的统计；

b） 实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；
c） 实际环境中的监测数据发现的威胁极其频率的统计；
d） 近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。

6.4 脆弱性识别（含已有控制措施）

6.4.1 脆弱性识别

脆弱性本身不会造成损害，它被某个威胁所利用才会造成损害。如果脆弱性没有对应的威胁，则无需实施控制措施，但应注意并监视他们是否发生变化。应注意，控制措施的不合理实施、控制措施故障或控制措施的误用本身也是脆弱性。控制措施因其运行的环境，可能有效或无效。相反，如果威胁没有对应的脆弱性，也不会导致风险。

脆弱性可从管理和技术两个方面进行审视。管理脆弱性与拟投保组织整体管理环境有关，管理脆弱性识别以拟投保组织为单位，一个拟投保组织做一次管理脆弱识别；技术脆弱性与具体技术活动相关，技术脆弱性识别以信息系统为单位，一个信息系统做一次技术脆弱性识别。

脆弱性识别针对保险标的识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估。表7提供了一种脆弱性识别方法。

表7 脆弱性识别方法

类型	识别类	识别项
管理脆弱性（组织层面）	安全管理	管理制度
		组织机构
		人员安全
		意识培训
		外包商管理
		供应链管理
		资产管理
		漏洞管理
		邮件管理
		定期评估
		应急响应
		备份恢复
		合规评估
技术脆弱性（信息系统层面）	安全防护	物理安全
		边界防护
		安全审计
		访问控制
		身份鉴别
		入侵防范
	监测预警	上网行为监测
		恶意代码监测
		情报应用

注：根据保险业务开展特性，脆弱性识别（已有安全控制措施）内容采用“是否”提问方式进行。在脆弱性赋值时，若识别相关脆弱性的存在，则赋予对应权重分值。附录A提供了脆弱性识别内容的详细清单。

6.4.2 赋予系数值

在进行业务板块识别时，根据测评项的重要性，分别对其设置不同系数值，为后续计算风险分值时提供参照依据。

6.4.3 已有安全控制措施识别

已有安全控制措施确认与脆弱性识别存在内在的联系。详见附录B已有安全控制措施确认表。

7 网络安全保险通用场景风险计算

结合网络安全保险风险评估的实际情况，对业务（重要性）、资产（重要性）、威胁（威胁动机、威胁能力、威胁频率）、脆弱性（结合已有安全控制措施）分别进行计算，最终得出一个具体的风险分值（0-100分之间），并在风险分值的基础上，再划分风险等级，风险分值与风险等级用于评判、衡量拟投保保险标的网络安全风险状况。

7.1 业务风险计算

对已经识别的业务板块、及某一业务板块下承载的信息系统，根据其重要性，分别赋予不同的权重值，表8提供了一种针对业务权重赋值的参考。

表8 权重赋值方法

等级	标识	权重值（百分比）	描述
5	很高	100%	业务或业务流程在战略中极其重要，在战略的属性及职能定位层面具有重大影响，在战略的发展目标层面中短期目标或长期目标中占据极其重要的地位，在业务规划层面与较多业务交叉性强，是多个业务流程的重要环节。
4	高	100~70（含）%	业务或业务流程在战略中较为重要，在战略的属性及职能定位层面具有较大影响，在战略的发展目标层面中短期目标或长期目标中占据极其重要的地位，在业务规划层面与较多业务交叉性存在交叉性。
3	中等	70~40（含）%	业务或业务流程在战略中具有一定重要性，在战略的属性及职能定位层面具有一定影响，在战略的发展目标层面中短期目标或长期目标中占据重要的地位，在业务规划层面与其他业务存在一定交叉性。
2	低	40~20（含）%	业务或业务流程在战略中具有一定重要性，在战略的属性及职能定位层面具有较低影响，在战略的发展目标层面中短期目标或长期目标中占据一定的地位，在业务规划层面与其他业务存在较小的交叉性。
1	很低	20~0%	业务或业务流程在战略中具有一定重要性，在战略的属性及职能定位层面具有较低影响，在战略的发展目标层面中短期目标或长期目标中占据较低的地位，在业务规划层面相对独立。

7.2 资产风险计算

7.2.1 系数值

根据业务重要程度，资产分为5个级别（第5级最高），业务重要程度越高，以及对资产的依赖程度越高，资产价值就越大，如表9所示。

表9 资产分级与价值系数

等级	标识	系数值	描述
5	很高	1	非常重要，其安全属性破坏后造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；
4	高	0.98	重要，其安全属性破坏后造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

表9　资产分级与价值系数（续）

等级	标识	系数值	描述
3	中等	0.95	比较重要，其安全属性破坏后造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；
2	低	0.9	不太重要，其安全属性破坏后造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。
1	很低	0.8	不重要，其安全属性破坏后对组织造成导很小的损失，甚至忽略不计

7.2.2　权重

某一信息系统下承载的所有资产，根据其重要性分别赋予权重值（与被评估方沟通，并得到认可），具体的权重赋值方法可参考表8。

7.3　威胁风险计算

威胁等级可划分为5个级别（第5级最高）。根据每种威胁依据威胁动机、威胁能力、威胁频率，采用加权平均方式（依据威胁程度，权值建议采用不同权值）。在实际的评估中，威胁的判断依据应根据历史统计或行业判断予以确定，并得到被评估方的认可，如表10所示。

表10　威胁系数表

等级	标识	系数值	定义
5	很高	1	威胁很高
4	高	0.98	威胁高
3	中等	0.95	威胁中等
2	低	0.9	威胁低
1	很低	0.8	威胁几乎不可能发生

7.4　脆弱性（含已有控制措施）风险计算

7.4.1　计算步骤

计算分成以下几个步骤：

a)　计算管理脆弱性分值，在组织层面对脆弱性做整体风险识别并得出管理脆弱性分值；
b)　将管理脆弱性分值转换为对应的系数值；
c)　计算技术脆弱性分值，在信息系统层面对脆弱性做风险识别并赋值，该信息系统承载的资产统一继承信息系统的脆弱性赋值；
d)　计算整体脆弱性分值，整体脆弱性分值=管理脆弱性分值对应的系数值×技术脆弱性分值。

7.4.2　计算公式

计算公式如下所示：

$$V=\sum_{k=1}^{n}\frac{100\times Wk\times Xk}{n} \quad \cdots\cdots (1)$$

式中：

V——脆弱性风险分值
n——测评项数
Wk——权重，
Xk——测评分值

表11为权重表，将某一测评项根据重要性划分三档权重值，“一般测评指标”权重0.4、“重要测评指标”权重0.7、“关键测评指标”权重1。

表12为测评结果分值表，该表中“测评结果”值为附录B已有安全性措施选项得分；“得分”值为附录B已有安全性措施实施效果得分。分成三档：是（达到要求）0分，（部分达到要求）0.5分、否（未达到要求）1分。

表11　三档权重值

指标重要性	权重
一般测评指标	0.4
重要测评指标	0.7
关键测评指标	1

表12　测评分值

测评结果	得分	说明
是（达到要求）	0分	1、“测评结果”值为附录B已有安全性措施选项 2、“得分”值为附录B已有安全性措施实施效果得分 3、如同一测评项目，遇到多个对象的，所有对象结果不一致时，最后结果是“部分达到要求”，这里不按少数服从多数来取最后的结果，例如：达到要求、部分达到要求、部分达到要求→部分达到要求，而不是未到达要求。
部分达到要求	0.5分	
否（未达到要求）	1分	
不适用	不计入公式中	

7.4.3　脆弱性分值（含已有控制措施）

经过识别、分析计算出的脆弱性分值对应脆弱性的5个级别（第5级最高），如表14所示：

表13　脆弱性分值与分级

等级	标识	分值	与分值对应的系数值（用于管理脆弱性变换）
5	很高	100~90（含）	1
4	高	90~80（含）	0.98
3	中等	80~70（含）	0.95
2	低	70~60（含）	0.9
1	很低	<60	0.8

7.5　风险分值的计算

7.5.1　风险分值计算步骤

风险分值计算步骤如下：

a)　计算资产风险分值：以某资产为单位，计算风险分值；

b)　计算信息系统风险分值：各资产风险分值加权平均后，得出这些资产承载的某信息系统的风险分值；

c)　计算业务板块风险分值：某业务板块承载的各信息系统，加权平均后计算风险分值；

d)　计算投保标的物风险分值：各业务板块风险分值加权平均后，计算投保标的物的风险分值。

7.5.2　风险分值计算公式

风险分值计算公式如下：

a)　计算安全事件发生可能性：

$$L = \sqrt{T \times V} \quad \cdots\cdots (2)$$

式中：

L——安全事件发生的可能性

T——威胁系数值（发生频率）
V——脆弱性分值（严重程度）

b） 计算安全事件的损失

$$F = \sqrt{La \times V} \quad (3)$$

式中：

F——安全事件损失
La——资产系数值（发生频率）
V——脆弱性分值（严重程度）

c） 计算安全事件风险分值

$$R = L \times F \quad (4)$$

式中：

R——安全事件风险分值
L——安全事件发生可能性
F——安全事件损失

7.5.3 风险分值与风险等级

a） 通用场景的风险分值、风险等级与核保建议

经过上述风险评估全部流程，最终计算的风险分值和风险等级、核保之间的对应关系，如表14所示。

表14 风险分值与风险等级、核保之间的对应关系

风险等级	风险分值	内容描述	核保建议
特别重大风险	100~90（含）	被测对象中存在极严重的安全问题，需要立即整改	不建议承保
重大风险	90~60（含）	被测对象中存在较严重的安全问题，需要立即加固	加固后承保
中等风险	60~20（含）	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险	加固后承保
一般风险	20~10（含）	被测对象中存在安全问题，但不会导致被测对象面临高、中等级安全风险	加固后承保
低风险	10~0（含）	被测对象安全风险较小	建议承保

b） 包含主要险种的风险分值、风险等级与承保建议

风险分值=通用场景的风险分值+典型场景的风险分值

注：典型场景的风险值计算见第8章，风险等级、核保建议见表14。

8 网络安全保险典型场景风险计算

网络安全保险典型场景包含以下三类：数据安全场景、网络勒索场景、业务连续性中断场景。

8.1 数据安全场景

8.1.1 概述

数据安全场景的风险可被网络安全保险大类中第一方损失和第三者责任项下责任承保，保险险别包含且不限于：应急服务+数据修复责任、外包商数据安全责任、数据安全责任等。

8.1.2 资产识别

数据安全场景的风险评估资产识别按照第6.2条开展。

8.1.3 威胁识别

数据安全场景的风险评估威胁识别按照第6.3条开展。

8.1.4 脆弱性识别（含已有控制措施）

数据安全场景的风险评估脆弱性识别（含已有控制措施）除了按照第6.4条开展外，还应识别表15中所列出的扩展识别项及内容。

表15　数据安全场景脆弱性识别扩展项

类型	识别类	识别项	识别内容	权重
管理脆弱性（组织层面）	安全管理	管理制度	是否有健全的数据安全管理办法和规范。（可覆盖数据安全全生命周期）	1
		组织机构	是否聘任首席合规官、数据保护主管或法务长以负责数据保护相关事宜?	
		定期评估	是否定期开展数据安全风险评估。	
			是否定期开展个人信息安全影响评估。	
		应急响应	是否具有针对数据泄露、数据破坏等数据安全事件场景下的专项应急预案。	
		备份恢复	是否备份了适用的驱动程序或应用程序安装文件（与备份，软件许可协议等一起存储）	
			是否定期检测备份恢复系统功能有效性	
	数据安全	数据分类分级	是否开展数据分类分级工作。	
			是否制定数据分类分级策略、方法及制度。	
			是否有数据发现及数据识别工具或产品。	
		数据采集	是否在数据采集时告知用户数据采集目的及用途，并最小化采集数据。	
			是否符合合法性及正当性要求。	
			是否在数据采集时按照统一标准及要求，规范数据入库操作。	
			是否对数据源进行身份鉴别和记录，并对数据进行标识?	
		数据存储	是否对重要业务信息、系统数据、软件系统等对象具备并维持本地备份及恢复程序。	
			是否定期执行数据备份和恢复。	
			是否与数据存储平台系统管理人员签订保密协议。	
			是否按照数据访问权限管理制度和数据存储安全策略，针对不同数据存储平台系统配备对用户或业务（是否用程序）的访问控制措施，确保非授权用户或业务（是否用程序）不能访问数据。	
		数据处理	是否使用未脱敏的数据用于业务系统的开发测试。	
			是否完整记录数据使用过程中的操作日志。	
			数据导出是否有明确的安全评估和授权审批流程。	
		数据传输	是否采取加密、脱敏、去标识化等技术手段保护重要数据、敏感数据及个人信息等的安全。	
			重要数据（包括但不限于鉴别数据、重要业务数据和重要个人信息等）在传输过程中是否采用密码技术保证其机密性。	
			重要数据（包括但不限于鉴别数据、重要业务数据和重要个人信息等）在传输过程中是否采用校验技术或密码技术保证其完整性。	
			是否建立相应审批流程，对跨组织机构或使用互联网的数据传输事项进行前置审批。	
		数据交换	是否在隐私政策中允许与第三方共享数据。	
			是否提供对外的数据接口。	
			是否定期对本企业对外数据接口进行清查，对不符合要求的对外数据接口立刻予以关停。	
		数据销毁	是否建立针对重要数据的删除、净化机制。	

表15　数据安全场景脆弱性识别扩展项（续）

类型	识别类	识别项	识别内容	权重
			是否建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程，留存审批记录至少不少于6个月。	
			是否对数据的批量销毁采用双人操作模式，单人不得拥有完整操作权限。	
		数据审计	是否有针对数据库记录、数据安全产品日志的审计。	
			是否针对数据全生命周期各阶段开展审计。	
			是否有数据库审计系统等审计工具或产品。	
		安全运营	是否有数据泄露防护产品或数据运营平台	

注：“数据安全”识别类及其对应的识别项均为新增加。

8.2　网络勒索场景

8.2.1　概述

网络勒索场景的风险可被网络安全保险大类中的第一方损失项下责任承保，保险险别包含且不限于：网络勒索威胁和勒索支付费用责任。

8.2.2　业务识别

网络勒索场景的风险评估业务识别按照第6.1条开展。

8.2.3　资产识别

网络勒索场景的风险评估资产识别按照第6.2条开展。

8.2.4　威胁识别

网络勒索场景的风险评估威胁识别按照第6.3条开展。

8.2.5　脆弱性识别（含已有控制措施）

网络勒索场景的风险评估脆弱性识别（含已有控制措施）除了按照第6.4条开展外，还应识别表16中所列出的扩展识别项及内容。

表16　网络勒索场景脆弱性识别扩展项

类型	识别类	识别项	识别内容	权重
管理脆弱性（组织层面）	安全管理	管理制度	是否建立了网络安全勒索情报的收集、处理、管理机制	1
			是否建立针对网络勒索事件的报送机制和对外信息共享、联动机制	
		意识培训	是否开展了网络勒索防范的专项培训，其中包括有关如何识别和报告可疑活动或事件的方法（例如网络钓鱼）	
			是否在组织范围内进行过网络钓鱼测试，以评估员工的安全意识，增强识别潜在恶意电子邮件的能力	
		邮件管理	是否实施了基于域的邮件身份验证策略	
		应急响应	是否制定了专门针对网络勒索场景的应急响应制度和流程	
			是否开展过组织层面的网络勒索专项应急演练	
		备份恢复	是否备份了适用的驱动程序或应用程序安装文件（与备份，软件许可协议等一起存储）	
			是否定期检测备份恢复系统功能有效性	

表16　网络勒索场景脆弱性识别扩展项（续）

类型	识别类	识别项	识别内容	权重
技术脆弱性（信息系统层面）	安全防护	入侵防范	是否对弱口令做监测	1
			是否已通过禁用或修改默认端口的形式防范远程登录风险	
	监测预警	恶意代码监测	是否采取技术措施防止并阻断勒索软件在组织内部的传送和传播	
			是否在所有资产上实施应用程序控制，以确保只运行授权的软件和进程，并且阻止所有未经授权的软件行？？？？	
			是否采取技术措施检测勒索软件及其他恶意软件	

8.3　业务连续性中断场景

8.3.1　概述

业务连续性中断场景的风险可被网络安全保险大类中的第一方损失项下责任承保，保险险别包含且不限于：营业中断损失责任（包含营业收入损失、从属营业收入损失、利润损失等）。

8.3.2　业务识别

业务连续性中断场景的风险评估业务识别按照第6.1条开展。

8.3.3　资产识别

业务连续性中断场景的风险评估资产识别按照第6.2条开展。

8.3.4　威胁识别

业务连续性中断场景的风险评估威胁识别除了按照第6.3条开展以外，需重点关注表17所列威胁：

表17　业务连续性中断场景威胁识别扩展项

编号	威胁源	威胁描述	威胁等级	资产	威胁系数值
1	拒绝服务攻击	攻击服务器使业务无法响应正常访问	很高	应用服务器	1
2	分布式拒绝服务攻击	多个攻击者同时向业务系统发动攻击，耗尽系统资源导致业务无法访问			
3	勒索攻击	加密业务数据导致无法正常使用，并索取赎金		数据库服务器	

8.3.5　脆弱性识别（含已有控制措施）

业务连续性中断场景风险评估脆弱性识别（含已有控制措施）除了按照第6.4条开展外，还应识别表18中所列出的扩展识别项及内容。

表18　业务连续性中断场景脆弱性识别扩展项

类型	识别类	识别项	识别内容	权重
管理脆弱性（组织层面）	安全管理	应急响应	是否有针对服务器故障、业务系统故障、重要网络设备故障等场景导致重要业务连续性中断的专项应急预案	1
			是否有针对防护设备误拦截正常业务导致连续性中断的应急预案	
		备份恢复	是否备份了适用的驱动程序或应用程序安装文件（与备份，软件许可协议等一起存储）	
			是否定期检测备份恢复系统功能有效性	
技术脆弱性（信息系统层面）	安全防护	物理安全	是否设置冗余或并行的电力电缆线路为计算机系统供电	

表18　业务连续性中断场景脆弱性识别扩展项（续）

类型	识别类	识别项	识别内容	权重
			是否提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求	
		边界防护	是否提供关键边界防护设备的硬件冗余	
			是否存在可以直接中断关键业务会话的特征匹配规则	
	监测预警	恶意代码监测	是否将关键业务进程设定为防病毒白名单	

8.4 典型场景风险值计算

$$R = \frac{L1}{l} \times R1 + \frac{L2}{l} \times R2 + \frac{L3}{l} R3 \cdots\cdots (5)$$

式中：

R——典型场景风险分值
R1——数据安全场景风险分值
R2——网络勒索场景风险分值
R3——业务连续性中断场景风险分值
L1——数据安全场景险种赔偿限额
L2——网络勒索场景险种赔偿限额
L3——业务连续性中断场景险种赔偿限额
1——保单赔偿限额

附 录 A
（资料性）
脆弱性识别表

脆弱性识别与权重赋值如表A.1所示。

表A.1 脆弱性识别内容

类型	识别类	识别项	识别内容	权重
管理脆弱性（组织层面）	安全管理	管理制度	是否建立了网络安全策略总体方针和安全策略文档；	1
			是否实施相应策略和流程以确保遵守网络安全法、行业法律法规或合同要求；	1
			是否通过正式、有效的方式传达组织管理制度给组织内部员工和外部相关方；	0.7
		组织机构	是否设置主管信息安全管理工作的职能部门，并设立系统管理员、网络管理员、审计管理员等岗位和岗位职责；	1
		人员安全	内/外部人员离职或离场后，是否及时终止外部访问人员的所有访问权限？	1
			外部人员物理访问、接入受控网络访问系统前是否有明确的审批流？	1
		意识培训	是否每年至少对员工开展一次全员安全意识教育培训；	0.4
			是否针对安全岗位人员每年至少开展一次安全技能培训和考试；	0.4
		外包商管理	是否将任一部分的网络、计算机系统开发或信息安全工作委托外包作业？	0.4
			是否将数据搜集及/或数据处理委托外包作业？	0.4
			是否建立了外包商信息安全管理策略？（包括但不限于数据使用等管理规范、外包商遴选/管理方式及流程等）	1
			是否对外包商及其提供的服务进行定期监控评价，确保其遵循企业的信息安全策略？	0.7
		供应链管理	是否有供应链安全管理制度，经审核后发布并定期更新；	0.7
			是否有供应商选择和管理策略，能根据产品和服务重要程度对供应商开展安全调查；	0.7
			是否与选定的供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务，明确提供者的安全责任并作出必要安全承诺，由于供应商原因导致发生网络安全事件，是否承担相应赔偿责任；	0.7
			是否采取技术手段对系统接入的供应商信息系统进行授权；	0.7
			授权接入的供应商信息系统在接入前是否开展安全评估，包括但不限于是否存在恶意代码、漏洞、后门等方面的安全评估；	0.7
			系统集成商和外部服务提供商是否能定期对供应链核心系统进行安全风险自审或引入第三方审计；	0.7
		资产管理	是否编制、保存与投保系统关联的资产清单（如计算机软硬件、网络设备安全设备等）	0.4
			是否在定期或在重大变化时更新维护资产清单？	0.4
		漏洞管理	是否指定或授权专人，定期对组织资产进行漏洞检测，并将检测结果做好记录、存档；	0.7
			是否能发现可能存在的已知漏洞，支持CVE\CNNVD\CNCVE\CNVD4种（任一）漏洞库编号；	0.7
			是否对发现的安全漏洞及时进行修补或评估可能的影响后进行修补，确保漏洞补丁经过测试后才可使用；	0.7

表A.1 脆弱性识别内容（续）

类型	识别类	识别项	识别内容	权重
			是否实现对网内资产漏洞信息进行统一关联、展现和告警；	0.7
			是否及时整改上级单位下发漏洞通告，并对其他潜在问题彻底全面排查；	0.7
		邮件管理	是否在关键网络节点处部署邮件防护相关产品或技术措施，并配置防范策略。	0.7
			是否能定期升级和更新防护规则库	0.7
		定期评估	是否定期执行常规/全面的安全检查以改进信息安全风险防护水平；	0.4
			是否定期开展信息安全管理方面的内、外部审计；	0.4
			是否定期开展数据安全风险评估工作；	0.7
			系统上线前是否进行了安全性测试；（全新上线或变更上线）	0.7
		应急响应	是否根据国家、行业或地方有关部门应急管理相关规定，制定网络安全事件应急预案；	0.7
			是否对安全事件应急预案定期进行演练；	0.7
			是否明确运营网络涉及到的系统和设备供营商应急服务责任，并在相关协议中规定；	0.7
			是否有聘请外部专家队伍，保障安全事件得到及时有效处置；	0.7
		备份恢复	是否提供重要数据的本地数据备份与恢复功能；	0.7
			是否提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	0.7
			是否提供重要数据处理系统的热冗余，保证系统的高可用性。	0.7
		合规评估	是否符合《信息安全技术网络安全等级保护基本要求》对应等级保护要求；	1
			是否符合《关键信息基础设施安全保护条例》防护能力要求；	1
			是否符合《信息系统密码是否用测评要求》相关要求；	1
			是否符合所属行业网络安全相关要求；	1
技术脆弱性（信息系统层面）	安全防护	物理安全	是否有定义需要保护的物理区域（如机房、财务部门等）；	0.7
			是否针对物理安全区域有人员访问控制；	0.7
			是否设置机房防盗监控机制；	0.4
		边界防护	是否对网络进行了区域划分，并合理分配网络地址；	0.7
			是否在重要网络区域与其他网络区域之间（如内外网）部署了网闸、防火墙和设备访问控制列表(ACL)等可靠的技术隔离手段；	0.7
			是否建立并限制无线网络的使用；	0.7
		安全审计	是否启用安全审计功能，对是否用系统所有用户操作进行审计；	0.7
			是否保存运维操作日志至少6个月以上；	0.7
			是否定期备份审计日志；	0.7
			是否对远程运维具有严格的审批流程；	0.4
		访问控制	是否使用Telnet不安全的远程运维方式；	0.7
			是否通过堡垒机或防火墙、安全域等对终端接入范围进行限制；	0.7
		身份鉴别	是否存在弱口令；（针对投保系统所有关联资产，包括但不限于终端、服务器、网络设备、安全设备、数据库、中间件、业务是否用系统）	0.7

表A.1 脆弱性识别内容（续）

类型	识别类	识别项	识别内容	权重
			是否重命名或删除默认账户；（针对投保系统所有关联资产，包括但不限于终端、服务器、网络设备、安全设备、数据库、中间件、业务是否用系统）	1
			员工账号是否有分类分级；	1
			是否配置并启用了登录失败处理功能、登录连接超时及自动退出功能；（针对投保系统所有关联资产，包括但不限于终端、服务器、网络设备、安全设备、数据库、中间件、业务是否用系统）	0.4
		入侵防范	是否关闭了非必要的系统服务和默认共享，且不存在非必要的高危端口（如445、135、139等）；	1
			是否限制并要求用户安装正版软件；	1
			是否限定了u盘、移动硬盘等外接设备使用，并关闭自动播放功能；	1
			是否有补丁推送更新机制？（计算机终端及所有服务器）	1
			是否采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析？	0.4
	监测预警	上网行为监测	是否具有上网行为管理设备?	0.7
			是否定期检查违反规定无线上网及其他违反网络安全策略的行为?	0.7
		恶意代码监测	是否计算机终端及所有服务器使用防毒保护及程序以防护及阻止病毒、计算机蠕虫、间谍程序及其它恶意程序?	1
			是否具备防病毒网关或统一威胁管理平台（UTM)恶意代码库？	1
		情报应用	是否有获取最新漏洞和安全事件情报信息的途径？	0.4
			是否会在获取最新漏洞或事件情报后，对资产情况进行排查和加固？	0.7

附 录 B
（资料性）
已有安全控制措施识别表

已有安全控制措施识别与赋值表如表B.1所示。

表B.1 已有安全控制措施识别内容

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
管理脆弱（组织层面）	安全管理	管理制度	是否建立了网络安全策略总体方针和安全策略文档；	是/否	0/1	
			是否实施相应策略和流程以确保遵守网络安全法、行业法律法规或合同要求；	是/否	0/1	
			是否通过正式、有效的方式传达组织管理制度给组织内部员工和外部相关方；	是/否	0/1	
		组织机构	是否设置主管信息安全管理工作的职能部门，并设立系统管理员、网络管理员、审计管理员等岗位和岗位职责；	是/部分达到要求/否	0/0.5/1	1、无负责部门为1分； 2、有负责部门，人员为专职或兼职0.5分2、有负责部门，人员为专职且有副总以上级别的公司领导全面主管为0分
		人员安全	内/外部人员离职或离场后，是否及时终止外部访问人员的所有访问权限？	是/否	0/1	
			外部人员物理访问、接入受控网络访问系统前是否有明确的审批流？	是/否	0/1	
		意识和培训	是否每年至少对员工开展一次全员安全意识教育培训；	是/部分达到要求/否	0/0.5/1	至少对员工开展一次全员安全意识教育培训、增加场景类的安全意识测评各占0.5分
			是否针对安全岗位人员每年至少开展一次安全技能培训和考试	是/部分达到要求/否	0/0.5/1	
		外包商管理	是否将任一部分的网络、计算机系统开发或信息安全工作委托外包作业？	是/部分达到要求/否	1/0.5/0	只要有任何外包即为0.5分
			是否将数据搜集及/或数据处理委托外包作业？	是/部分达到要求/否	1/0.5/0	数据搜集、数据处理各占0.5分
			是否建立了外包商信息安全管理策略？（包括但不限于数据使用等管理规范、外包商遴选/管理方式及流程等）	是/否	0/1	
			是否对外包商及其提供的服务进行定期监控评价，确保其遵循企业的信息安全策略？	是/否	0/1	
		供应链管理	是否有供应链安全管理制度，经审核后发布并定期更新；	是/否	0/1	
			是否有供应商选择和管理策略，能根据产品和服务重要程度对供应商开展安全调查；	是/否	0/1	

表 B.1 已有安全控制措施识别内容（续）

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
			是否与选定的供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务，明确提供者的安全责任并作出必要安全承诺，由于供应商原因导致发生网络安全事件，是否承担相应赔偿责任；	是/否	0/1	
			是否采取技术手段对系统接入的供应商信息系统进行授权；	是/否	0/1	
			授权接入的供应商信息系统在接入前是否开展安全评估，包括但不限于是否存在恶意代码、漏洞、后门等方面的安全评估？	是/否	0/1	
			系统集成商和外部服务提供商是否能定期对供应链核心系统进行安全风险自审或引入第三方审计？	是/否	0/1	
		资产管理	是否编制、保存与投保系统关联的资产清单（如计算机软硬件、网络设备安全设备等）	是/部分达到要求/否	0/0.5/1	1、是，主要是靠行政或采购等部门梳理出的固定资产清单得0.5分； 2、是，资产清单内容包括了资产范围(含设备设施、软件、文档等)、资产责任部门、重要程度和所处位置等的0分
			是否在定期或在重大变化时更新维护资产清单？	是/否	0/1	
		漏洞管理	是否指定或授权专人，定期对组织资产进行漏洞检测，并将检测结果做好记录、存档；	是/否	0/1	
			是否能发现可能存在的已知漏洞，支持CVE\CNNVD\CNCVE\CNVD4种（任一）漏洞库编号；	是/否	0/1	只要有任一漏洞库编号即为1分
			是否对发现的安全漏洞及时进行修补或评估可能的影响后进行修补，确保漏洞补丁经过测试后才可使用；	是/否	0/1	
			是否实现对网内资产漏洞信息进行统一关联、展现和告警；	是/否	0/1	
			是否及时整改上级单位下发漏洞通告，并对其他潜在问题彻底全面排查；	是/否	0/1	
		邮件管理	是否在关键网络节点处部署邮件防护相关产品或技术措施，并配置防范策略。	是/否	0/1	防垃圾邮件网关或组件
			是否能定期升级和更新防护规则库	是/否	0/1	

表 B.1 已有安全控制措施识别内容（续）

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
		定期评估	是否定期执行常规/全面的安全检查以改进信息安全风险防护水平；	是/部分达到要求/否	0/0.5/1	至少每季度进行常规安全检查，检查内容包括：1、安全运维报告（系统日常运行状态、数据备份等），2、漏洞检测等安全测试内容（请提供评估报告）。每一项得0.5分
			是否定期开展信息安全管理方面的内、外部审计；	是/部分达到要求/否	0/0.5/1	内部审计、外部审计各占0.5分
			是否定期开展数据安全风险评估工作；	是/否	0/1	
			系统上线前是否进行了安全性测试；（全新上线或变更上线）	是/否	0/1	
		应急响应	是否根据国家、行业或地方有关部门应急管理相关规定，制定网络安全事件应急预案；	是/否	0/1	
			是否对安全事件应急预案定期进行演练；	是/否	0/1	
			是否明确运营网络涉及到的系统和设备供营商是否应急服务责任，并在相关协议中规定；	是/部分达到要求/否	0/0.5/1	只要有供应商有相关协议得0.5分
			是否有聘请外部专家队伍，保障安全事件得到及时有效处置；	是/否	0/1	
		备份恢复	是否提供重要数据的本地数据备份与恢复功能；	是/部分达到要求/否	0/0.5/1	
			是否提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	是/部分达到要求/否	0/0.5/1	
			是否提供重要数据处理系统的热冗余，保证系统的高可用性。	是/部分达到要求/否	0/0.5/1	
		合规评估	是否符合《信息安全技术网络安全等级保护基本要求》对应等级保护要求；	是/否	0/1	
			是否符合《关键信息基础设施安全保护条例》防护能力要求；	是/否	0/1	
			是否符合《信息系统密码是否用测评要求》相关要求；	是/否	0/1	
			是否符合所属行业网络安全相关要求；	是/否	0/1	
技术脆弱性	安全防护	物理安全	是否有定义需要保护的物理区域（如机房、财务部门等）？	是/否	0/1	
			是否针对物理安全区域有人员访问控制？	是/部分达到要求/否	0/0.5/1	纸质记录访问人员信息0.5分；配置电子门禁系统，鉴别和记录进入人员信息为0分

表 B.1 已有安全控制措施识别内容（续）

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
			是否设置机房防盗监控机制？	是/部分达到要求/否	0/0.5/1	安装视频监控系统，持续记录为0.5分；安装防盗报警系统，或在安装视频监控系统的同时安排专人进行值守为0分
		边界防护	是否对网络进行了区域划分，并合理分配网络地址？	是/否	0/1	
			是否在重要网络区域与其他网络区域之间（如内外网）部署了网闸、防火墙和设备访问控制列表(ACL)等可靠的技术隔离手段？	是/部分达到要求/否	0/0.5/1	网闸、防火墙和设备访问控制列表(ACL)缺一，即为0.5分
			是否建立并限制无线网络的使用？	是/部分达到要求/否	0/0.5/1	1、有授权的无线网络被单独组网后接入到有线网络，并部署无线网关接入网关无线网络控制器等设备，使用WPA2加密方式，强口令设置，并部署非授权无线设备管控措施，如无线嗅探器、无线入侵检测/防御系统、手持式无线信号检测系统等即为0分；2、上述缺一即为0.5分；3、未建立限制无线网络使用的即为1分
		安全审计	是否启用安全审计功能，对应用系统所有用户操作进行审计？	是/否	0/1	
			是否保存运维操作日志至少6个月以上？	是/否	0/1	
			是否定期备份审计日志？	是/部分达到要求/否	0/0.5/1	存储记录6个月以下的即为0.5分
			是否对远程运维具有严格的审批流程？	是（或无远程运维）/部分达到要求/否	0/0.5/1	1、使用了规定的端口或通道，具备审批程序和记录，但不保留远程运维执行操作的审计日志（请提供证明）即为0.5分；2、使用了规定的端口或通道，具备审批程序和记录，具备远程运维执行操作的审计日志（请提供证明）即为0.5分。

表 B.1 已有安全控制措施识别内容（续）

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
		访问控制	是否使用Telnet不安全的远程运维方式？	是/部分达到要求/否	1/0.5/0	1、选择QQ、Teamviewer等第三方软件即为0.5分；2、使用VPN即为0分
			是否通过堡垒机或防火墙、安全域等对终端接入范围进行限制？	是/否	0/1	
		身份鉴别	是否存在弱口令？（针对投保系统所有关联资产，包括但不限于终端、服务器、网络设备、安全设备、数据库、中间件、业务应用系统）	是/部分达到要求/否	0/0.5/1	1、采用了双因素以上措施，且其中一种采用了密码技术，如调用了密码机或采取SM1-SM4等算法即为0分；使用堡垒机进行统一管理即为0分；2、口令长度8为以内，可包含数字、字母和符号，无强制更换周期即为1分；3、介于上述两者之间的即为0.5分
			是否重命名或删除默认账户？（针对投保系统所有关联资产，包括但不限于终端、服务器、网络设备、安全设备、数据库、中间件、业务应用系统）	是/部分达到要求/否	0/0.5/1	1、已重命名或删除默认账户即为0.5分；2、已重命名或删除默认账户，并修改默认账户的默认口令即为0分
			员工账号是否有分类分级？	是/部分达到要求/否	0/0.5/1	1、不同职位的员工，账号权限不同，遵循最小权限和职责分离即为0分；2、无明确规定账号权限即为1分；3、介于两者之间的为0.5分
			是否配置并启用了登录失败处理功能、登录连接超时及自动退出功能？（针对投保系统所有关联资产，包括但不限于终端、服务器、网络设备、安全设备、数据库、中间件、业务应用系统）	是/部分达到要求/否	0/0.5/1	1、启动了登录失败处理功能；设置了合理的连接超时自动断开的等待时间，若长时间无操作，系统设置了符合业务需求的结束会话时间即为0分；2、启动了登录失败处理功能，如限制非法登录次数，超过预定错误次数时，系统锁定，由管理员解锁或过一段时间后自动解锁即为0.5分

表 B.1 已有安全控制措施识别内容（续）

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
		入侵防范	是否关闭了非必要的系统服务和默认共享，且不存在非必要的高危端口（如445、135、139等）？	是/否	0/1	
			是否限制并要求用户安装正版软件？	是/否	0/1	
			是否限定了u盘、移动硬盘等外接设备使用，并关闭自动播放功能？	是/部分达到要求/否	0/0.5/1	1、已限制只允许特定的外接设备可以使用即为0.5分；2、关闭自动播放即为0.5分；3、限制外接设备的使用，并关闭自动播放功能即为0分
			是否有补丁推送更新机制？（计算机终端及所有服务器）	是/否	0/1	
			是否采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析？	是/部分达到要求/否	0/0.5/1	1、有威胁情报检测系统、抗DDoS攻击系统或入侵保护系统即为0分；2、有上述任一项的即为0.5分
	监测预警	上网行为监测	是否具有上网行为管理设备?	是/否	0/1	
			是否定期检查违反规定无线上网及其他违反网络安全策略的行为?	是/否	0/1	
		恶意代码监测	是否计算机终端及所有服务器使用防毒保护及程序以防护及阻止病毒、计算机蠕虫、间谍程序及其它恶意程序?	是/部分达到要求/否	0/0.5/1	定期或遇重大更新及时安排即为0分；定期手动即为0.5分
			是否具备防病毒网关或统一威胁管理平台（UTM)恶意代码库？	是/否	0/1	
		情报应用	是否有获取最新漏洞和安全事件情报信息的途径？	是/部分达到要求/否	0/0.5/1	1、从多个渠道获取，并结合安全服务商所提供的内容即为0分；2、公司内部人员自行进行情报收集和判断或者从互联网漏洞平台或安全设备厂商获取即为0.5分
			是否会在获取最新漏洞或事件情报后，对资产情况进行排查和加固？	是/部分达到要求/否	0/0.5/1	1、是，解决部分问题或关键问题，如存在无法解决的情况则不再跟进即为0.5分；2、是，跟进并编制问题跟踪表形成闭环机制即为0分

附 录 C
（资料性）
典型场景已有安全控制措施识别

C.1 数据安全场景已有安全控制措施识别

表C.1 数据安全场景已有安全控制措施识别表

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
管理脆弱（组织层面）	安全管理	管理制度	是否有健全的数据安全管理办法和规范？（可覆盖数据安全全生命周期）	是/否	0/1	
		组织机构	是否聘任首席合规官、数据保护主管或法务长以负责数据保护相关事宜；	是/部分达到要求/否	0/0.5/1	专职为1分，兼职为0.5分,无为1分
		定期评估	是否定期开展数据安全风险评估	是/否	0/1	
			是否定期开展个人信息安全影响评估	是/否	0/1	
		应急响应	是否具有针对数据泄露、数据破坏等数据安全事件场景下的专项应急预案。	是/否	0/1	
		备份恢复	是否备份了适用的驱动程序或应用程序安装文件（与备份，软件许可协议等一起存储）	是/否	0/1	
			是否定期检测备份恢复系统功能有效性	是/否	0/1	
	数据安全	数据分类分级	是否开展数据分类分级工作。	是/否	0/1	
			是否制定数据分类分级策略、方法及制度。	是/部分达到要求/否	0/0.5/1	
			是否有数据发现及数据识别工具或产品。	是/否	0/1	
		数据采集	是否在数据采集时告知用户数据采集目的及用途，并最小化采集数据？	是/否	0/1	
			是否符合合法性及正当性要求？	是/否	0/1	
			是否在数据采集时按照统一标准及要求，规范数据入库操作？	是/否	0/1	
			是否对数据源进行身份鉴别和记录，并对数据进行标识？	是/否	0/1	
		数据存储	是否对重要业务信息、系统数据、软件系统等对象具备并维持本地备份及恢复程序。	是/否	0/1	
			是否定期执行数据备份和恢复。	是/否	0/1	
			是否与数据存储平台系统管理人员签订保密协议。	是/否	0/1	
			是否按照数据访问权限管理制度和数据存储安全策略，针对不同数据存储平台系统配备对用户或业务（是否用程序）的访问控制措施，确保非授权用户或业务（是否用程序）不能访问数据。	是/否	0/1	
		数据处理	是否使用未脱敏的数据用于业务系统的开发测试。	是/否	0/1	
			是否完整记录数据使用过程中的操作日志。	是/部分达到要求/否	0/0.5/1	本地备份即为0.5分；异地备份即为0分
			数据导出是否有明确的安全评估和授权审批流程。	是/否	0/1	

表C.1　数据安全场景已有安全控制措施识别表（续）

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
			是否采取加密、脱敏、去标识化等技术手段保护重要数据、敏感数据及个人信息等的安全。	是/否	0/1	
		数据传输	重要数据（包括但不限于鉴别数据、重要业务数据和重要个人信息等）在传输过程中是否采用密码技术保证其机密性。	是/否	0/1	
			重要数据（包括但不限于鉴别数据、重要业务数据和重要个人信息等）在传输过程中是否采用校验技术或密码技术保证其完整性。	是/否	0/1	
		数据交换	是否建立相应审批流程，对跨组织机构或使用互联网的数据传输事项进行前置审批。	是/否	0/1	
			是否在隐私政策中允许与第三方共享数据。	是/否	0/1	
			是否提供对外的数据接口。	是/部分达到要求/否	1/0.5/0	提供接口，且定义数据接口安全策略；与数据接口调用方签署合作协议，明确数据安全责任；提供数据接口调用提供身份鉴别和访问控制，提供异常处理能力、接口访问审计能力；提供数据接口调用提供身份鉴别和访问控制，提供异常处理能力、接口访问审计能力即为0分
			是否定期对本企业对外数据接口进行清查，对不符合要求的对外数据接口立刻予以关停。	是/否	0/1	
		数据销毁	是否建立针对重要数据的删除、净化机制。	是/否	0/1	
			是否建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程，留存审批记录至少不少于6个月。	是/否	0/1	
			是否对数据的批量销毁采用双人操作模式，单人不得拥有完整操作权限。	是/否	0/1	
		数据审计	是否有针对数据库记录、数据安全产品日志的审计。	是/部分达到要求/否	0/0.5/1	
			是否针对数据全生命周期各阶段开展审计。	是/部分达到要求/否	0/0.5/1	
			是否有数据库审计系统等审计工具或产品	是/否	0/1	
		安全运营	是否有数据泄露防护产品或数据运营平台	是/部分达到要求/否	0/0.5/1	

C.2 网络勒索场景已有安全控制措施识别

表C.2 网络勒索场景已有安全控制措施识别表

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
管理脆弱（组织层面）	安全管理	管理制度	是否建立了网络安全勒索情报的收集、处理、管理机制	是/否	0/1	
			是否建立针对网络勒索事件的报送机制和对外信息共享、联动机制	是/部分达到要求/否	0/0.5/1	专职为1分，兼职为0.5分,无为1分
		意识培训	是否开展了网络勒索防范的专项培训，其中包括有关如何识别和报告可疑活动或事件的方法（例如网络钓鱼）	是/否	0/1	
			是否在组织范围内进行过网络钓鱼测试，以评估员工的安全意识，增强识别潜在恶意电子邮件的能力	是/否	0/1	
		邮件管理	是否实施了基于域的邮件身份验证策略	是/否	0/1	
		应急响应	是否制定了专门针对网络勒索场景的应急响应制度和流程	是/否	0/1	
			是否开展过组织层面的网络勒索专项应急演练	是/否	0/1	
		备份恢复	是否备份了适用的驱动程序或应用程序安装文件（与备份，软件许可协议等一起存储）	是/否	0/1	
			是否定期检测备份恢复系统功能有效性	是/否	0/1	
技术脆弱性（信息系统层面）	安全防护	入侵防范	是否对弱口令做监测	是/否	0/1	
			是否已通过禁用或修改默认端口的形式防范远程登录风险	是/否	0/1	
	监测预警	恶意代码监测	是否采取技术措施防止并阻断勒索软件在组织内部的传送和传播	是/否	0/1	
			是否在所有资产上实施应用程序控制，以确保只运行授权的软件和进程，并且阻止所有未经授权的软件行	是/否	0/1	
			是否采取技术措施检测勒索软件及其他恶意软件	是/否	0/1	

C.3 业务连续性中断场景已有安全控制措施识别

表C.3 业务连续性中断场景已有安全控制措施识别表

风险分类	控制类	控制子类	脆弱性	已有控制措施	已有控制措施实施效果	说明
管理脆弱（组织层面）	安全管理	应急响应	是否有针对服务器故障、业务系统故障、重要网络设备故障等场景导致重要业务连续性中断的专项应急预案	是/否	0/1	
			是否有针对防护设备误拦截正常业务导致连续性中断的应急预案	是/否	0/1	
		备份恢复	是否备份了适用的驱动程序或应用程序安装文件（与备份，软件许可协议等一起存储）	是/否	0/1	
			是否定期检测备份恢复系统功能有效性	是/否	0/1	
技术脆弱性（信息系统层面）	安全防护	物理安全	是否设置冗余或并行的电力电缆线路为计算机系统供电	是/否	0/1	
			是否提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求	是/否	0/1	
		边界防护	是否提供关键边界防护设备的硬件冗余	是/否	0/1	
			是否存在可以直接中断关键业务会话的特征匹配规则	是/否	0/1	
	监测预警	恶意代码监测	是否将关键业务进程设定为防病毒白名单	是/否	0/1	

附 录 D
（资料性）
某虚拟银行 A 风险评估示例

D.1 概述

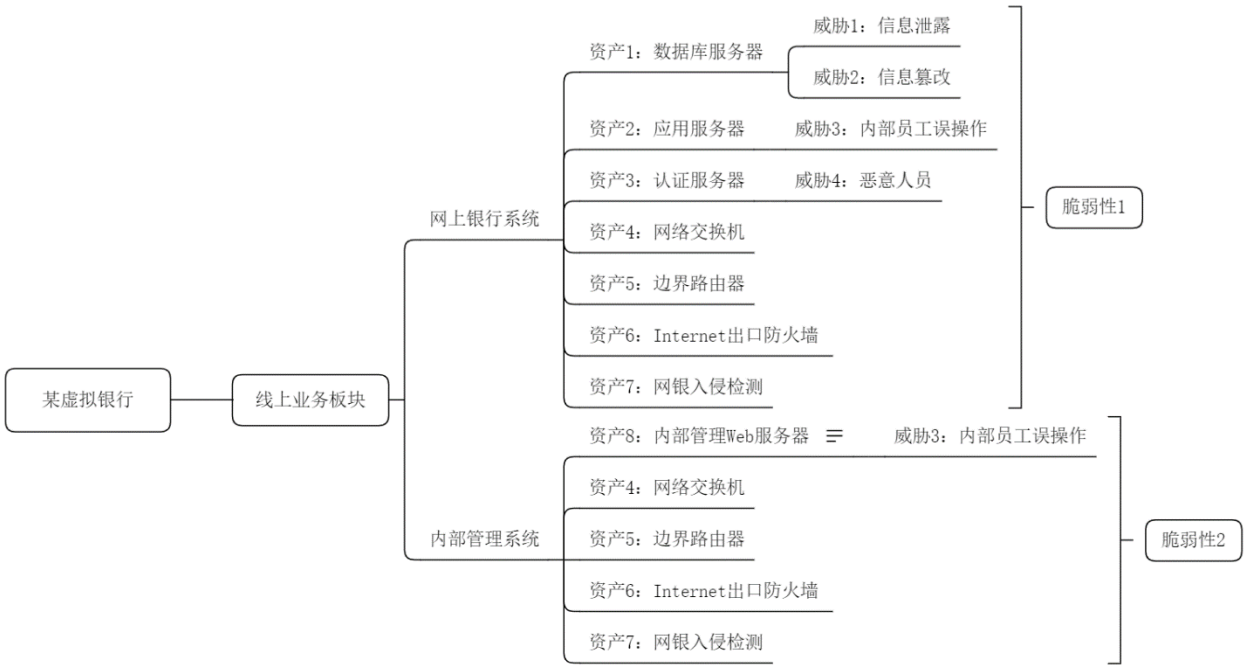
本章节将给出一个风险评估的示例，介绍如何对拟投保标的做风险评估，并得出风险分值和风险等级。评估对象是某虚拟银行A的线上业务板块（包含网上银行系统、内部管理系统）。

a) 本案例中假定评估人员已经完成资产调查工作；

b) 为简化步骤，将风险识别与赋分值结合在一起。

D.2 资产图谱

根据资产调整工作情况，给出资产图谱：



图D.1 资产图谱

D.3 风险识别

D.3.1 业务识别

业务识别可以分成三个步骤：一是识别出组织拟投保的业务板块，承载各业务的信息系统数量、类型；二是对业务板块、信息系统做风险单位划分；三是对业务板块、信息系统的重要性赋予不同的权重。

第一步：该虚拟银行A拟投保标的为线上业务板块，该板块由两个信息系统组成，分别为网上银行系统、内部管理系统。

第二步：因拟投保标的为一个线上业务板块，可以将该板块划分为一个风险单位。

第三步：经与甲方客户交流沟通，根据信息系统承载业务的重要性，拟将网上银行系统权重设置为80%，内部管理系统权重为20%。

表D.1 A 银行业务板块及信息系统

编号	业务板块	信息系统	权重
1	线上业务板块	网上银行系统	80%
		内部管理系统	20%

D.3.2 资产识别

资产识别主要有两个方面的内容：一是识别出各信息系统承载的资产数量、类型等；二是根据资产重要性赋予不同的系数值。具体见下表：

表D.2 A网上银行系统主要资产

编号	主机名	操作系统	IP地址	说　　明	主要应用	资产类型	资产系数值	权重
1	数据库服务器	AIX 5.2	192.168.1.100	网银系统的数据库服务器。	Oracle	主机资产	1	60%
2	应用服务器	AIX 5.2	192.168.1.101	网银系统的应用服务器。	websphere	主机资产	1	15%
3	认证服务器	定制的Debian Linux	192.168.1.105	用于专业版用户和企业用户的证书认证。	PKI服务	主机资产	1	15%
4	网络交换机	三层网络交换设备	192.168.1.104	YYY-0001-ZZZ	网银业务系统的三层网络交换机	网络设备资产	0.98	2.5%
5	边界路由器	路由器	192.168.1.106	YYY-0002-ZZZ	网银系统的边界路由设备	边界路由设备	网络设备资产	0.98
6	Internet出口防火墙	防火墙	192.168.1.102	出口防火墙	为系统提供网络访问控制，并为相关服务器提供网络地址转换服务。	安全设备	0.98	2.5%
7	网银入侵检测	N序号S	192.168.1.103	入侵检测设备	为整个网银系统提供入侵检测服务。	安全设备	0.98	2.5%

表D.3 A内部管理系统主要资产

编号	主机名	操作系统	IP地址	说　　明	主要应用	资产类型	资产系数值	权重
1	内部管理Web服务器	Windows2000	192.168.1.104	网银柜台管理人员对交易进行审核、管理的Web服务器，只允许从银行的内部网络进行访问。	IIS、ASP	主机资产	1	90%
2	网络交换机	三层网络交换设备	192.168.1.104	YYY-0001-ZZZ	网银业务系统的三层网络交换机	网络设备资产	0.98	2.5%
3	边界路由器	路由器	192.168.1.106	YYY-0002-ZZZ	网银系统的边界路由设备	网络设备资产	0.98	2.5%
4	Internet出口防火墙	防火墙	192.168.1.102	出口防火墙	为系统提供网络访问控制，并为相关服务器提供网络地址转换服务。	安全设备	0.98	2.5%
5	网银入侵检测	N序号S	192.168.1.103	入侵检测设备	为整个网银系统提供入侵检测服务。	安全设备	0.98	2.5%

D.3.3 威胁识别

表D.4 A网上银行系统主要威胁

编号	资产	威胁源	威胁等级	威胁系数值
1	数据库服务器	信息泄露	很高	1
		信息篡改	高	0.98
2	应用服务器	内部员工误操作	中等	0.95

表D.4　A网上银行系统主要威胁（续）

编号	资产	威胁源	威胁等级	威胁系数值
3	认证服务器	恶意人员	中等	0.95

表D.5 A 内部管理系统主要威胁

编号	资产	威胁源	威胁等级	威胁系数值
1	内部管理 web服务器	内部员工误操作	高	0.98

D.3.4　脆弱性识别（含已有安全控制措施）

①　脆弱性识别从管理脆弱性（组织层面）、技术脆弱性（信息系统层面）两个维度做识别。

②　根据附录B脆弱性识别表中识别类、识别项、识别内容进行脆弱性识别；

③　根据附录C已有安全控制措施表中已有安全控制措施、已有安措施实施效果、说明对脆弱性进行赋分值。

④　计算脆弱性=管理脆弱性系数值×技术脆弱性分值。

表D.6 A 网上银行系统脆弱性

编号	资产	脆弱性类别	脆弱性分值	脆弱性系数值	说明
1	网上银行系统	管理脆弱性（组织层面）	60分	0.9	每个投保标的物管理脆弱性只需要评估一次
		技术脆弱性（信息系统层面）	65分	-	技术脆弱性是以信息系统为单位评估并计算分值

注：网上银行系统脆弱性=管理脆弱性系数值×技术脆弱性分值=0.9×65分=58.5分

表D.7 A 内部管理系统脆弱性

编号	资产	脆弱性类别	脆弱性分值	脆弱性系数值	说明
1	内部管理系统	管理脆弱性（组织层面）	50分	0.8	每个投保标的物管理脆弱性只需要评估一次
		技术脆弱性（信息系统层面）	65分	-	技术脆弱性是以信息系统为单位评估并计算分值

注：内部管理系统脆弱性=管理脆弱性系数值×技术脆弱性分值=0.8×65分=52分

D.4　风险分值计算

a)　以资产 1 作为示例，计算风险分值：

资产 1：数据库服务器、威胁 1、脆弱性 1 安全事件风险分值=安全事件发生可能性×安全事件损失

$=\sqrt{威胁\ 1\ 系数值 \times 脆弱性分值} \times \sqrt{资产系数值 \times 脆弱性分值}$

$=\sqrt{1 \times 58.5} \times \sqrt{1 \times 58.5}$

=58.5分

资产 1：数据库服务器、威胁 2、脆弱性 1 安全事件风险分值=安全事件发生可能性×安全事件损失

$=\sqrt{威胁\ 2\ 系数值 \times 脆弱性分值} \times \sqrt{资产系数值 \times 脆弱性分值}$

$=\sqrt{0.98 \times 58.5} \times \sqrt{1 \times 58.5}$

=57.9分

资产1：最终安全事件风险分值=（威胁1对应的风险分值+威胁2对应的风险分值）/2

=（58.5+57.9）/2
=58.2分

同理，计算其他资产安全事件风险分值：

表D.8 A 网上银行系统

资产	风险分值	资产权重
资产1：数据库服务器	58.2分	60%
资产2：应用服务器	57.12分	15%
资产3：认证服务器	57.12分	15%
资产4：网络交换机	-	2.5%
资产5：边界路由器	-	2.5%
资产6：Internet出口防火墙	-	2.5%
资产7：网银入侵检测	-	2.5%

表D.9 A 内部管理系统

资产	风险分值	资产权重
资产8：数据库服务器	51.48分	90%
资产4：网络交换机	-	2.5%
资产5：边界路由器	-	2.5%
资产6：Internet出口防火墙	-	2.5%
资产7：网银入侵检测	-	2.5%

b） 各资产风险分值加权平均后，得出这些资产承载的某信息系统的风险分值；

表D.10 风险分值计算

信息系统	风险分值	说明
网上银行系统	52.06分	资产1、资产2、资产3、资产4、资产5、资产6、资产7加权平均
内部管理系统	46.33分	资产8、资产4、资产5、资产6、资产7加权平均

c） 某业务板块承载的各信息系统，加权平均后计算风险分值；

线上业务板块风险分值 = 网上银行系统风险分值×权重+内部管理系统风险分值×权重
= 52.06×80%+46.33×20%
= 41.65+9.27
= 50.92分

d） 各业务板块风险分值加权平均后，计算拟投保保险标的的风险分值。

因本案例只有一个业务板块，所以该投保标的最终风险分值就以线上业务板块风险分值为主。

查表风险等级为中等风险。

参 考 文 献

[1] ISO/IEC FDIS 27102 Information security management Guidelines for cyber insurance
[2] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南
[4] GB/T 31722-2015 信息技术 安全技术 信息安全风险管理
[5] GB/T 36466-2018 信息安全技术 工业控制系统风险评估实施指南
[6] GB/T 36637-2018 信息安全技术 ICT供应链安全风险管理指南
[7] GB/T 37988-2019信息安全技术 数据安全能力成熟度模型
[8] 信息安全技术 关键信息基础设施安全防护能力评价方法（征求意见稿）