ICS 35.020
CCS L 70

DB3212

泰 州 市 地 方 标 准

DB3212/T 1117—2022

政务数据安全风险评估规范

Government Data Security Risk Assessment Specification

2022-12-28 发布　　2022-12-28 实施

泰州市市场监督管理局　发布

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。

本文件由泰州市大数据管理局提出。

本文件由泰州市大数据管理局归口。

本文件起草单位：泰州市大数据管理局、泰州市标准化院。

本文件主要起草人：陈书剑、王小冬、孙慧、刘小芳、赵文涛、梁鑫晨、许鑫、施驰乐、吴薇、陈蓝生、张婧娴、李海鹏、郭健、王友成。

政务数据安全风险评估规范

1 范围

本文件提供了政务数据安全风险评估的评估原则、风险评估框架及流程、风险评估实施等要求。

本文件适用于政务数据安全的风险评估。

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 信息安全风险评估方法

GB/T 25069 信息安全技术 术语

GB/T 37973 信息安全技术 大数据安全管理指南

DB32/T 3421 基础地理信息安全系统安全风险评估规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务数据 government data

各级政务部门在履行职责过程中依法采集、生成、存储、管理的各类数据资源。

注：根据可传播范围，政务数据一般包括可共享政务数据、可开放公共数据及不宜开放共享政务数据。

3.2

数据安全 data security

指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.3

风险评估 risk assessment

风险识别、风险分析和风险评价的整个过程。

3.4

数据安全风险评估 data security risk assessment

是指从风险管理角度，运用科学的方法与手段，根据数据分类分级情况，系统分析数据所面临的安全威胁，以及可能遭受的危害程度，有针对性地提出抵御数据安全威胁的防护对策和措施。

3.5

安全威胁 security Threat

可能对系统或组织的数据处理活动造成危害的因素，其形式可以是对数据直接或间接的攻击，在数据机密性、完整性和可用性等方面造成损害，也可能是偶发的或蓄意的事件。

3.6

安全脆弱性 security vulnerability

通过利用数据安全威胁，导致数据在处理活动中的安全属性被破坏的薄弱环节。

4 风险评估原则

政务数据安全风险评估的基本原则包括：

a) 安全保障性原则。不应因风险评估造成基础地理信息数据的泄露、篡改和删除，保障数据的安全性；
b) 人员可控性原则。所有参与评估人员应签署保密协议，以保证项目信息的安全；
c) 信息可控性原则。评估方应对工作过程数据和结果数据严格管理，未经授权不得泄露给任何单位和个人；
d) 过程可控性原则。按照项目管理要求，成立风险评估项目实施团队，并实行项目组长负责制，达到项目过程的可控；
e) 工具可控性原则。评估人员所使用的评估工具应事先告知用户，并在评估实施前获得被评估方的许可。

5 风险评估框架及流程

5.1 风险要素关系

风险评估中基本要素的关系如图 1 所示。风险评估基本要素包括资产、威胁、脆弱性和安全措施，并基于以上要素开展风险评估。

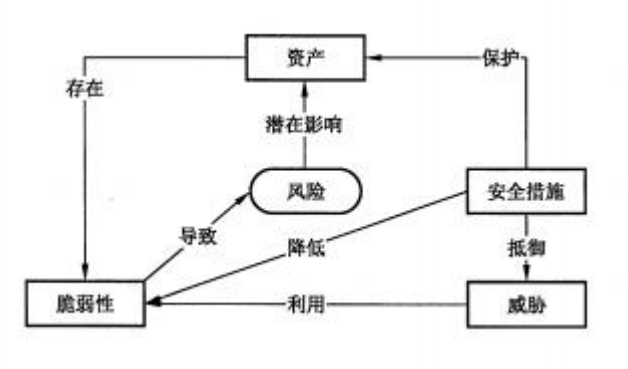

图 1 风险评估基本要素之间关系

5.2 风险分析原理

风险分析原理如下：

a) 根据威胁的来源、种类、动机等，并结合威胁相关安全事件、日志等历史数据统计，确定威胁的能力和频率；
b) 根据脆弱性访问路径、触发要求等，以及已实施的安全措施及其有效性确定脆弱性被利用难易程度；
c) 确定脆弱性被威胁利用导致安全事件发生后对资产所造成的影响程度；
d) 根据威胁的能力和频率,结合脆弱性被利用难易程度，确定安全事件发生的可能性；
e) 根据资产在发展规划中所处的地位和资产的属性，确定资产价值；
f) 根据影响程度和资产价值，确定安全事件发生后对评估对象造成的损失；
g) 根据安全事件发生的可能性以及安全事件造成的损失，确定评估对象的风险值；
h) 依据风险评价准则,确定风险等级，用于风险决策。

5.3 风险评估流程

风险评估的实施流程如图 2 所示。风险评估流程应包括如下内容。

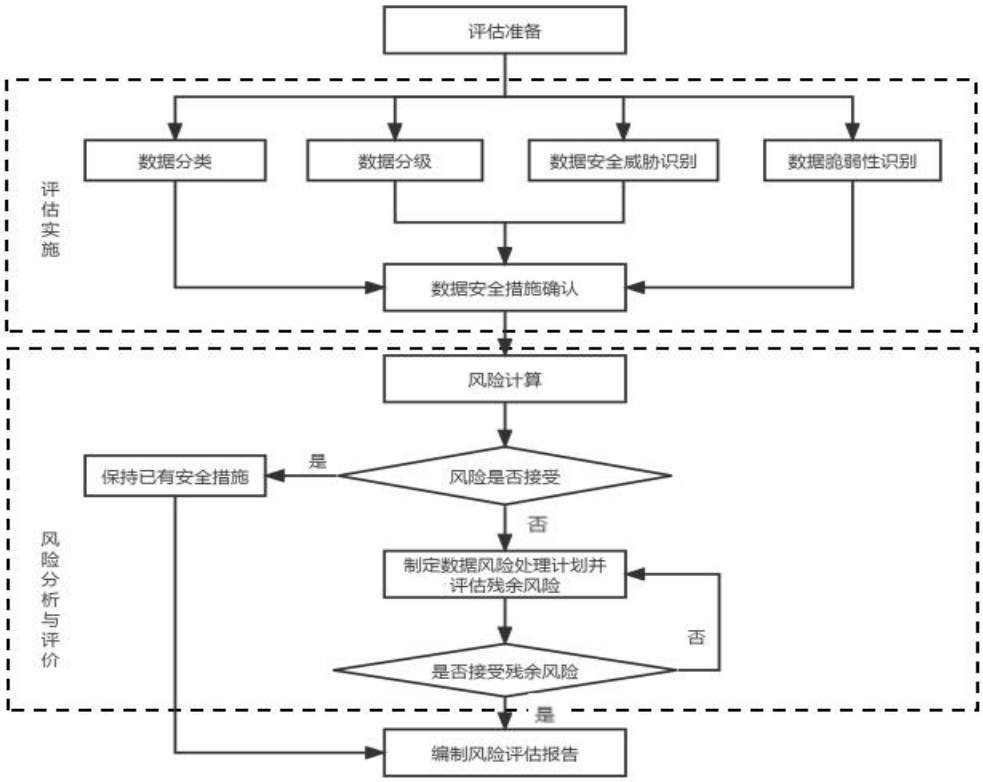

图 2 风险评估实施流程图

a) 评估准备，此阶段应包括：
   1) 确定风险评估的目标；
   2) 确定风险评估的对象、范围和边界；
   3) 组建评估团队；
   4) 开展前期调研；
   5) 确定评估依据；
   6) 建立风险评价准则；
   7) 制定评估方案。
b) 评估实施，此阶段应包括：
   1) 政务数据分类；
   2) 政务数据分级；
   3) 政务数据安全威胁识别；
   4) 政务数据脆弱性识别；
   5) 政务数据安全措施确认。
c) 风险分析与评价，此阶段应包括：
   1) 风险分析计算；
   2) 风险评估；
   3) 风险接受程度；
   4) 风险处置措施。
d) 编制报告。此阶段应包括处理的重要数据的种类、数量，开展数据处理活动情况，面临数据安全风险及其对应措施等。

6 风险评估实施

6.1 评估准备

组织实施风险评估是一种战略性的考虑，其结果将受到组织规划、业务、业务流程、安全需求、系统规模和结构等方面的影响。因此，在风险评估实施前应准备以下工作。

a) 在考虑风险评估的工作形式、在生命周期中所处阶段和被评估单位的安全评估需求的基础上，确定风险评估目标。附录 A 给出了评估对象生命周期各阶段的风险评估内容，附录 B 给出了风险评估的工作形式描述。
b) 确定风险评估的对象、范围和边界。
c) 组建评估团队、明确评估工具。附录 C 给出了风险评估的工具。
d) 开展前期调研。
e) 确定评估依据。
f) 建立风险评价准则：组织应在考虑国家法律法规要求及行业背景和特点的基础上，建立风险评价准则，以实现对风险的控制与管理。
   风险评价准则应满足以下要求：
   1） 符合组织的安全策略或安全需求；
   2） 满足利益相关方的期望；
   3） 符合组织业务价值。
   建立风险评价准则的目的包括但不限于：
   1） 对风险评估的结果进行等级化处理；
   2） 能实现对不同风险的直观比较；
   3） 能确定组织后期的风险控制策略。
g） 制定评估方案。
h） 评估方案需得到主管单位的支持和批准。

6.2 评估实施

6.2.1 数据分类

6.2.1.1 根据组织的政务数据安全需求以及相关法律法规的规定，按照组织政务数据安全管理的目标和原则，组织定期梳理重要政务数据处理活动有关情况，形成重要政务数据目录。

6.2.1.2 根据政务数据在经济社会发展中的重要程度，以及遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对政务数据实行分类保护。

6.2.1.3 可参照各地区、各部门以及相关行业、领域按照分保分灰保护制度确定的重要政务数据具体目录。

6.2.2 数据识别

6.2.2.1 识别内容

系统资产识别包括资产分类和业务承载性识别两个方面。表 1 给出了系统资产识别的主要内容描述。系统资产分类包括信息系统、数据资源和通信网络，业务承载性包括承载类别和关联程度。

表 1　系统资产识别表

识别内容	示例
分类	信息系统：信息系统是指由计算机硬件、计算机软件、网络和通信设备等组成的，并按照一定的应用目标和规则进行信息处理或过程控制的系统。典型的信息系统如门户网站、业务系统、云计算平台、工业控制系统等 数据资源：数据是指任何以电子或者非电子形式对信息的记录。数据资源是指具有或预期具有价值的数据集。在进行数据资源风险评估时，应将数据活动及其关联的数据平台进行整体评估。数据活动包括数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等 通信网络：通信网络是指以数据通信为目的，按照特定的规则和策略，将数据处理结点、网络设备设施互连起来的一种网络。将通信网络作为独立评估对象时，一般是指电信网、广播电视传输网和行业或单位的专用通信网等以承载通信为目的的网络
业务承载性	承载类别：系统资产承载业务信息采集、传输、存储、处理、交换、销毁过程中的一个或多个环节关联程度：业务关联程度（如果资产遭受损害，将会对承载业务环节运行造成的影响，并综合考虑可替代性）、资产关联程度（如果资产遭受损害，将会对其他资产造成的影响，并综合考虑可替代性）

6.2.2.2　价值赋值

系统资产价值应依据资产的保密性、完整性和可用性赋值，结合业务承载性、业务重要性，进行综合计算，并设定相应的评级方法进行价值等级划分，等级越高表示资产越重要。表 2 中给出了系统资产价值等级划分的描述。资产保密性、完整性、可用性赋值以及业务承载性赋值方法见附录 D。

表 2　系统资产价值等级表

等级	标识	系统资产价值等级描述
5	很高	综合评价等级为很高，安全属性破坏后对组织造成非常严重的损失
4	高	综合评价等级为高，安全属性破坏后对组织造成比较严重的损失
3	中等	综合评价等级为中，安全属性破坏后对组织造成中等程度的损失
2	低	综合评价等级为低，安全属性破坏后对组织造成较低的损失
1	很低	综合评价等级为很低，安全属性破坏后对组织造成很小的损失，甚至忽略不计

6.2.2.3　组件和单元资产识别

系统组件和单元资产应分类识别，系统组件和单元资产分类包括系统组件、系统单元、人力资源和其他资产。表 3 给出了系统组件和单元资产识别的主要内容描述。

表 3　系统组件和单元资产识别表

分类	示例
系统单元	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 智能终端设备:感知节点设备（物联网感知终端）、移动终端等 网络设备:路由器、网关、交换机等 传输线路:光纤、双绞线等 安全设备:防火墙、入侵检测/防护系统、防病毒网关、VPN 等
系统组件	应用系统:用于提供某种业务服务的应用软件集合 应用软件:办公软件、各类工具软件、移动应用软件等 系统软件:操作系统、数据库管理系统、中间件、开发系统、语句包等 支撑平台：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 服务接口：系统对外提供服务以及系统之间的信息共享边界，如云计算 PassS 层服务向其他信息系统提供的服务接口等
人力资源	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：安全管理员、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
其他资产	保存在信息媒介上的各种数据资料:源代码、数据库数据、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 办公设备:打印机、复印机、扫描仪、传真机等 保障设备:UPS、变电设备、空调、保险柜、文件柜、门禁、消防设施等 服务:为了支撑业务、信息系统运行、信息系统安全,采购的服务等知识产权:版权、专利等

6.2.2.4　组件和单元资产赋值

系统组件和单元资产价值应依据其保密性、完整性、可用性赋值进行综合计算，并设定相应的评级方法进行价值等级划分,等级越高表示资产越重要。表 4 中给出了系组件和单元资产价值等级划分的描述。资产保密性、完整性、可用性赋值方法见附录 D。

表 4　系统组件和单元资产价值等级表

等级	标识	系统组件和单元资产价值等级描述
5	很高	综合评价等级为很高，安全属性破坏后对业务和系统资产造成非常严重的影响
4	高	综合评价等级为高,安全属性破坏后对业务和系统资产造成比较严重的影响
3	中等	综合评价等级为中,安全属性破坏后对业务和系统资产造成中等程度的影响
2	低	综合评价等级为低，安全属性破坏后对业务和系统资产造成较低的影响
1	很低	综合评价等级为很低，安全属性破坏后对业务和系统资产造成很小的影响,甚至忽略不计

6.2.3 政务数据分级

6.2.3.1 政务数据分级

按照表5政务数据分级判定标准可分为L1、L2、L3、L4四级，并根据就高性原则进行定级，报部门主要负责人审批同意。

表5 政务数据分级判定标准

判定等级	判定标识	判定标准
L4	涉密数据	涉及国家安全、国民经济、民生大事、军事机密等方面的数据；数据被破坏后，会对社会秩序和公共利益造成严重损害，或对国家安全造成损害。
L3	敏感数据	涉及个人或组织人身财产安全、公共利益、社会秩序等方面的数据；数据被破坏后，对公民、法人和其他组织的合法权益造成严重损害，或对社会秩序和公共利益造成损害，但不损害国家安全。
L2	受限数据	涉及个人或组织的基本信息、基本活动信息，可小范围内公开或有条件开放共享的数据；数据被破坏后，对公民、法人和其他组织的合法权益造成一般损害，但不损害国家安全、社会秩序和公共利益。
L1	公开数据	依法公开披露的数据；数据被破坏后，对社会秩序、公共利益以及对公民、法人和其它组织的合法权益均无影响。

6.2.4 安全威胁识别

6.2.4.1 威胁识别的内容包括威胁的来源、主体、种类、动机、时机和频率。

6.2.4.2 在对威胁进行分类前，应识别威胁的来源。威胁来源包括环境、意外和人为三类，附录D给出了威胁识别的参考方法。表6给出了一种威胁来源的分类方法。

6.2.4.3 根据威胁来源的不同，威胁可划分为信息损害和未授权行为等威胁种类。表6给出了一种威胁种类划分的参考。

表6 一种数据安全威胁分类方法

数据生命周期阶段	数据威胁分类	数据威胁描述
数据采集	恶意代码注入	数据入库时，恶意代码随数据注入到数据库或信息系统，危害数据机密性、完整性、可用性。
	数据无效写入	数据入库时，数据不符合规范或无效。
	数据污染	数据入库时，攻击者接入采集系统污染待写入的原始数据，破坏数据完整性。
	数据分类分级或标记错误	数据分类分级判断错误或打标记错误，导致数据受保护级别降低。
	数据源	不在目前的管理目录或者数据接口管理目录中，造成采集过期数据源或非法数据源。
	频度	不能否满足数据共享的要求，数据产生部门汇集数据与大数据管理平台采集数据频度不一致。
	数据范围	需求小于最初的数据共享范围，共享内容不合规。
数据传输	数据窃取	攻击者伪装成外部通信代理、通信对端、通信链路网关，通过伪造虚假请求或重定向窃取数据。
	数据监听	有权限的员工、第三方运维与服务人员接入，或攻击者越权接入内部通信链路与网关、通信代理监听数据。 攻击者接入外部通信链路与网关、通信代理、通信对端监听数据。
	数据篡改	攻击者伪装成通信代理或通信对端篡改数据。
数据存储	数据破坏	由于信息系统自身故障、物理环境变化或自然灾害导致的数据破坏，影响数据完整性和可用性。
	数据篡改	篡改网络配置信息、系统配置信息、安全配置信息、用户身份信息或业务数据信息等，破坏数据完整性和可用性。
	数据分类分级或标记错误	数据分类分级或相关标记被篡改，导致数据受保护级别降低。
	数据窃取	在数据库服务器、文件服务器、办公终端等对象上安装恶意工具窃取数据。
	恶意代码执行	故意在数据库服务器、文件服务器、办公终端等对象上安装恶意工具窃取数据。

	数据不可控	依托第三方云平台、数据中心等存储数据，没有有效的约束与控制手段。 在使用云计算或其他技术时，数据存放位置不可控，导致数据存储在境外数据中心，数据和业务的 司法管辖关系发生改变。
数据共享	共享数据未脱敏	与第三方机构共享数据时，第三方机构及其人员可以直接获取敏感元数据的调取、查看权限。
	共享权限混乱	与第三方机构共享数据时，接口权限混乱，导致第三方能访问其他未开放的数据。
	数据过度获取	由于业务对数据需求不明确，或未实现基于业务人员与所需要数据的关系的访问控制，业务人员 获取超过业务所需的数据，容易造成数据泄露。
	数据不可控	数据可被内部员工获取，组织对内部员工所获数据的保存、处理、再转移等活动不可控。 数据可被第三方服务商、合作商获取，组织对第三方机构及其员工所获薮据的使用、留存、再转移等活动未约束或不掌握，
数据加工	注入攻击	数据处理系统可能遭到恶意代码注入、SQL 注入等攻击，造成信息泄露，危害数据机密性、完整性、可用性。
	数据访问抵赖	人员访问数据后，不承认在某时刻用某账号访问过数据。
	使用权限混乱	处理系统调用数据接口权限混乱，导致能访问其他未开放的数据。
	数据过度获取	由于相关业务对数据需求不明确，或未实现基于业务人员、系统与所需数据的关系的访问控制，导致业务人员或处理系统获取超过业务所需数据， 容易造成数据泄露。
	数据不可控	依托第三方机构或外部处理系统处理数据，没有有效的约束与控制手段。
	敏感源数据未脱敏	处理系统可直接调取钺感元数据，容易导致信息泄露。
数据销毁	数据到期未销毁	数据失效或业务关闭后，遗留的敏感数据仍然可以被访问，破坏了数据的机密性。
	数据未正确销毁	被销毁数据通过技术手段可恢复，破坏了数据的机密性。

6.2.4.4 威胁主体依据人为和环境进行区分，人为的分为国家、组织团体和个人，环境的分为一般的自然灾害、较为严重的自然灾害和严重的自然灾害。

6.2.4.5 威胁动机是指引导、激发人为威胁进行某种活动，对组织业务、资产产生影响的内部动力和原因。 威胁动机可划分为恶意和非恶意，恶意包括攻击、破坏、窃取等，非恶意包括误操作、好奇心等。表 E.3 给出了一种威胁动机分类的参考。

6.2.4.6 威胁时机可划分为普通时期、特殊时期和自然规律。

6.2.4.7 威胁频率应根据经验和有关的统计数据来进行判断，综合考虑以下四个方面，形成特定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统计；
c） 实际环境中监测发现的威胁及其频率统计；
d） 近期公开发布的社会或特定行业威胁及其频率统计，以及发布的威胁预警。

6.2.4.8 威胁赋值

威胁赋值应基于威胁行为，依据威胁的行为能力和频率，结合威胁发生的时机，进行综合计算，并设定相应的评级方法进行等级划分，等级越高表示威胁利用脆弱性的可能性越大。表 7 中给出了威胁赋值等级划分的描述。

表 7　—种基于发生频率的数据安全威胁赋值方法

数据安全威胁频率	威胁赋值	数据安全威胁频率定义
很高	5	在该行业领域的业务系统中，通常不可避免的威胁，发生频率很高（或 N1 次/周）；或可以证实经常发生过。
高	4	在该行业领域的业务系统中，在多数情况下会发生的威胁，发生频率高（或 N1 次/月）；或可以证实多次发生过。
中等	3	在该行业领域的业务系统中，在特定条件下可能会发生的威胁，发生频率中等（或次/半年）；或被证实曾经发生过。
低	2	在该行业领域的业务系统中，一般不太容易发生的威胁，发生频率低；或没有被证实发生过。
很低	1	在该行业领域的业务系统中，很罕见和例外的情况下会发生的威胁，发生频率很低；或几乎不可能发生。

6.2.5　安全脆弱性识别

6.2.5.1　政务数据安全脆弱性识别是依据国际、国家安全标准或者行业规范、应用流程的安全要求，从管理与技术两个角度进行综合识别。当政务数据安全不能满足以下数据安全防护要求时，会产生政务数据安全脆弱性，评估人员应从以下方面进行数据安全脆弱性识别：

a)　政务数据采集：

1）　政务部门应根据本部门履行职责的需要依法采集信息，明确采集信息的范围、格式和采集流程，按照相关标准规范要求，在目录管理系统登记数据，确保数据真实、准确、完整和及时。

2）　各区委应根据自身实际情况，确定数据采集范围、数量和频度，确定采集过程中个人信息和重要数据的采集范围、控制措施。

3）　政务信息采集应遵循“源头采集、一数一源”的原则，凡可以通过共享获取的信息，各政务部门原则上不得要求自然人、法人或其他组织重复提交，法律、法规另有规定的除外。

4）　自然人数据应当以居民身份证号码作为标识进行采集，法人及其他组织数据应当以统一社会信用代码作为标识进行采集。

5）　政务部门应按相关技术标准对采集的政务数据开展数字化和结构化处理。对列入政务信息资源共享目录和开放目录的信息资源，未建设相应业务系统的，政务部门应按照相关技术标准积极开展业务系统建设，确保业务数据库与信息共享平台和数据开放平台之间的互联互通和同步更新。

6）　在数据抽取过程中使用到的中间账户应是专门为中台系统设计，且遵循“最小够用”原则。

7）　应记录并保存政务数据处理活动过程相关的信息。

8）　应对政务数据源和数据采集的环境、设施、技术采取必要的安全机制和管控措施，对产生数据的数据源进行身份鉴别和记录，确保采集数据的机密性、完整性和真实性。

b)　政务数据传输：

1）　数据传输过程中的身份鉴别技术应具备安全性，使得数据信息不会被非法操作或越权访问。

2）　确保数据传输应采用加密通道、元数据加密、去标识化、完整性校验或其他技术保证传输过程中的机密性和完整性，包括但不限于个人信息数据、业务信息数据、鉴别信息数据、日志信息数据等。

3）　应建立政务数据传输链路冗余机制，保证数据传输的可靠性和网络传输服务可用性。

c)　政务数据存储：

1）　政务部门应将政务信息资源统一存储到泰州市政务信息共享开放平台，加强数据存储前的保密审查，原则上机密级以下涉密数据通过全市电子政务内网平台承载，非涉密数据通过政务信息共享开放平台承载。

2） 政务数据存储应采用身份鉴别技术对数据访问者身份进行识别，确保数据在授权的安全范围内被使用、访问、操作，防止数据被任意读取，造成数据泄露或数据安全属性被破坏等后果。
3） 政务数据存储应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于个人信息数据、业务信息数据、鉴别信息数据、日志信息数据等。
4） 应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于业务信息数据、鉴别信息数据、日志信息数据等。
5） 应规定重要数据的备份方式、备份频度、存储介质、保存期等。
6） 应根据政务数据的重要性和政务数据对系统运行的影响，制定政务数据的备份和恢复策略、备份和恢复程序等。
7） 政务部门对政务数据涉密属性不明确或者有争议的，按照保密法有关规定执行。

d) 政务数据共享：
1） 涉及个人信息的政务数据开放内容，应根据业务对个人信息进行必要的去标识化处理。
2） 应能够检测开放数据资源是否含有非公开信息能力，确保公开数据合规。
3） 应具备对异常或高风险数据访问行为自动化识别和预警的能力，及时阻断违规行为。

e) 政务数据加工：
1） 应建立数据加工节点的安全机制，确保节点接入的真实性，防止数据泄露。
2） 在数据分析过程中对数据获取、访问接口、授权机制进行管控，应建立多源数据派生、聚合、关联分析过程的管控措施，避免分析结果泄露敏感数据、个人信息。
3） 应建立数据溯源机制，实现数据流向追踪，并对溯源数据进行保护。
4） 应建立数据加工再利用管控机制，确保对数据加工产生的组谷数据、关联数据、衍生数据的违规使用、未授权滥用、非法转存、跨境存储进行检测评估。

f) 政务数据销毁：
1） 应使用规范的工具或产品，采用可靠技术手段及时销毁符合销毁条件的数据，确保数据不可还原。
2） 对于数据存储介质的销毁，应使用国家权威机构认证的设备或国家认定资质的销毁服务提供商对存储介质设备进行物理销毁。

6.2.5.2 可根据政务数据的暴露程度、技术实现的难易程度、流行程度等，采用分级方式对数据安全脆弱性指数赋值，见表 8。

表 8 一种政务数据安全脆弱性指数与赋值方法

政务数据安全脆弱性指数	指数赋值	政务数据安全脆弱性指数程度定义
很高	5	如果政务数据安全脆弱性被利用，会对组织及其拥有的数据造成完全损害。
高	4	如果政务数据安全脆弱性被利用，会对组织及其拥有的数据造成重大损害。
中等	3	如果政务数据安全脆弱性被利用，会对组织及其拥有的数据造成较大损害。
低	2	如果政务数据安全脆弱性被利用，会对组织及其拥有的数据造成一般损害。
很低	1	如果政务数据安全脆弱性被利用，会对组织及其拥有的数据造成较小损害。

6.2.6 安全措施确认

6.2.6.1　在识别政务数据安全脆弱性的同时，评估人员应对数据安全措施的有效性进行评估确认。对有效的安全措施继续保持，对确认为不适当的安全措施应核实是否应被取消或对其进行修正，或用更合适的安全措施替代。

6.2.6.2　政务数据安全措施确认结果包括两种情况：

a)　防护措施对数据安全保障起到加强作用，此类防护措施应加以保持。

b)　对数据安全保障起到削弱作用，此类防护措施应被调整并予以加强。

6.2.6.3　政务数据安全措施调节因数。在对数据安全风险进行分析评价时，应考虑数据、数据安全威胁、数据安全脆弱性的综合作用以及数据安全措施产生的加强或削弱作用，因此引入数据安全措施调节因数对数据安全风险进行修正。

6.2.6.4　政务数据安全措施调节因数的取值应设置在一个合理的取值区间，能够反映现有数据安全措施对数据安全保障产生的加强或削弱作用。

6.3　风险分析与评价

6.3.1　应结合数据风险值计算和数据风险面临的风险等级对数据进行定量与定性的综合分析与评价。

6.3.2　应根据数据安全风险分析与评价过程应确定影响数据安全风险的要素、要素之间的组合方式以及具体的计算方法。影响数据安全风险的要素主要包括数据安全威胁频率、数据安全脆弱性指数、数据级别以及现有数据安全措施。

6.3.3　应根据安全威胁利用数据的脆弱性造成的破坏对数据安全风险进行评价。

6.4　编制报告

6.4.1　同时结合现有数据安全措施对数据安全风险的加强或削弱作用进行关联分析，并编制数据安全风险评估报告。

6.4.2　被评估组织根据本行业、单位的风险管理策略，确认数据安全风险接受程度，对不可接受的数据安全风险，应采取风险管控措施进行控制。

附 录 A
（资料性）
评估对象生命周期各阶段的风险评估

A.1 概述

风险评估应贯穿于评估对象生命周期各阶段中。评估对象生命周期各阶段中涉及的风险评估原则和方法是一致的，但由于各阶段实施内容、对象、安全需求不同，使得风险评估的对象、目的、要求等各方面也有所不同。在规划设计阶段，通过风险评估以确定评估对象的安全目标；在建设验收阶段，通过风险评估以确定评估对象的安全目标达成与否；在运行维护阶段，要持续的实施风险评估以识别评估对象面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现。因此，每个阶段风险评估的具体实施应根据该阶段的特点有所侧重的进行。

A.2 规划阶段的风险评估

规划阶段风险评估的目的是识别评估对象的业务规划，以支撑评估对象安全需求及安全规划等。规划阶段的评估应能够描述评估对象建成后对现有业务模式的作用，包括技术、管理等方面，并根据其作用确定评估对象建设应达到的安全目标。

本阶段评估中，资产、脆弱性不需要识别；威胁应根据未来应用对象、应用环境、业务状况、操作要求等方面进行分析。评估着重在以下几方面：

a） 是否依据相关规则，建立了与业务规划相一致的安全规划，并得到最高管理者的认可；

b） 是否依据业务建立与之相契合的安全策略，并得到最高安全管理者的认可；

c） 系统规划中是否明确评估对象开发的组织、业务变更的管理、开发优先级；

d） 系统规划中是否考虑评估对象的威胁、环境，并制定总体的安全方针；

e） 系统规划中是否描述评估对象预期使用的信息，包括预期的信息系统、资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；

D 系统规划中是否描述所有与评估对象安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、组织安全策略、专门技术和知识等。

规划阶段的评估结果应体现在评估对象整体规划或项目建议书中。

A.3 设计阶段的风险评估

设计阶段的风险评估需要根据规划阶段所明确的运行环境、业务重要性、资产重要性，提出安全功能需求设计阶段的风险评估结果应对设计方案中所提供的安全功能符合性进行判断，作为实施过程风险控制的依据。

本阶段评估中，应详细评估设计方案中面临威胁的描述，将评估对象使用的具体设备、软件等资产及其安全功能形成需求列表。对设计方案的评估着重在以下几方面：

a） 设计方案是否符合评估对象建设规划，并得到最高管理者的认可；

b） 设计方案是否对评估对象建设后面临的威胁进行了分析，重点分析来自物理环境和自然的威胁，以及由于内、外部入侵等造成的威胁；

c） 设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析，制定评估对象的总体安全策略；

d） 设计方案是否采取了一定的手段来应对可能的故障；

e） 设计方案是否对设计原型中的技术实现以及人员、组织管理等方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性；

f） 设计方案是否考虑随着其他系统接入而可能产生的风险；

g） 系统性能是否满足用户需求，并考虑到峰值的影响，是否在技术上考虑了满足系统性能要求的方法；

h） 应用系统（含数据库）是否根据业务需要进行了安全设计；

i） 设计方案是否根据开发的规模、时间及系统的特点选择开发方法，并根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

J）设计活动中所采用的安全控制措施、安全技术保障手段对风险的影响。在安全需求变更和设计变更后，也需要重复这项评估。

设计阶段的评估可以以安全建设方案评审的方式进行，判定方案所提供的安全功能与信息技术安全技术标准的符合性。评估结果应体现在评估对象需求分析报告或建设实施方案中。

A.4 实施阶段的风险评估

实施阶段风险评估的目的是根据安全需求和运行环境对系统开发、实施过程进行风险识别，并对建成后的安全功能进行验证。根据设计阶段分析的威胁和制定的安全措施，在实施及验收时进行质量控制。

基于设计阶段的资产列表、安全措施，实施阶段应对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，从而确定安全措施能否抵御现有威胁、脆弱性的影响。实施阶段风险评估主要对业务及其相关信息系统的开发、技术与产品获取，系统交付实施两个过程进行评估。开发、技术与产品获取过程的评估要点包括：

a） 法律、政策、适用标准和指导方针：直接或间接影响评估对象安全需求的特定法律；影响评估对象安全需求、产品选择的政府政策、国际或国家标准；

b） 评估对象的功能需要：安全需求是否有效地支持系统的功能；

c） 成本效益风险：是否根据评估对象的资产、威胁和脆弱性的分析结果，确定在符合相关法律、政策、标准和功能需要的前提下选择最合适的安全措施；

d） 评估保证级别：是否明确系统建设后应进行怎样的测试和检查，从而确定是否满足项目建设、实施规范的要求。

A.5 交付阶段的风险评估

系统交付实施过程的评估要点包括：

a） 根据实际建设的系统，详细分析资产、面临的威胁和脆弱性；

b） 根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁；

c） 评估是否建立了与整体安全策略一致的组织管理制度；

d） 对系统实现的风险控制效果与预期设计的符合性进行判断，如存在较大的不符合，应重新进行评估对象安全策略的设计与调整。

本阶段风险评估可以采取对照实施方案和标准要求的方式，对实际建设结果进行测试、分析。

A.6 运行阶段的风险评估

运行维护阶段风险评估的目的是了解和控制运行过程中的安全风险，是一种较为全面的风险评估。评估内容包括对真实运行的资产、威胁、脆弱性等各方面。

a）资产评估：包括对业务、系统资产、系统组件和单元资产的评估。业务评估包括业务定位、业务关联性、完整性、业务流程分析；系统资产评估包括系统分类和业务承载连续性的评估；系统组件和单元资产是在真实环境下较为细致的评估，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等，本阶段资产识别是前期资产识别的补充与增加。

b） 威胁评估：应全面地分析威胁的可能性和严重程度。对威胁导致安全事件的评估可以参照威胁来源动机、能力和安全事件的发生频率。

c） 脆弱性评估：是全面的脆弱性评估。包括运行环境中物理、网络、系统、应用、安全保障设备、管 理等各方面的脆弱性。技术脆弱性评估可以采取核查、扫描、案例验证、渗透性测试的方式实施；安全保障设备的脆弱性评估，应包括安全功能的实现情况和安全保障设备本身的脆弱性；管理脆弱性评估可以采取文档、记录核查等方式进行验证。

d） 风险计算：根据本文件的相关方法，对风险进行定性或定量的风险分析，描述不同业务、系统资产的风险高低状况。

运行维护阶段的风险评估应定期执行；当组织的业务流程、系统状况发生重大变更时，也应进行风险评估，重大变更包括以下情况（但不限于）：

a） 增加新的应用或应用发生较大变更；

b） 网络结构和连接状况发生较大变更；

c） 技术平台大规模的更新；

d） 系统扩容或改造；

e） 发生重大安全事件后，或基于某些运行记录怀疑将发生重大安全事件；

D 组织结构发生重大变动对系统产生了影响。

A.7 废弃阶段的风险评估

废弃阶段风险评估着重在以下几方面：

a） 确保硬件和软件等资产及残留信息得到了适当的处置，并确保系统组件被合理地丢弃或更换；

b） 如果被废弃的系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接，还需考虑系统废弃后与其他系统的连接是否被关闭；

c） 如果在系统变更中废弃，除对废弃部分外，还应对变更的部分进行评估，以确定是否会增加风险或引入新的风险；

d） 是否建立了流程，确保更新过程在一个安全、系统化的状态下完成。

本阶段应重点对废弃资产对组织的影响进行分析，并根据不同的影响制定不同的处理方式。对由于系统废弃可能带来的新的威胁进行分析，并改进新系统或管理模式。对废弃资产的处理过程应在有效的监督之下实施，同时对废弃的执行人员进行安全教育，评估对象的维护技术人员和管理人员均应参与此阶段的评估。

附 录 B
（资料性）
风险评估的工作形式

B.1 自评估

自评估是指评估对象的拥有、运营或使用单位发起的对本单位进行的风险评估。自评估应在本文件的指导下，结合评估对象特定的安全要求实施。周期性进行的自评估可以在评估流程上适当简化，重点针对自上次评估后评估对象发生变化后引入的新威胁，以及脆弱性的完整识别，以便于两次评估结果的对比。但评估对象发生 A.6 中所列的重大变更时，应依据本文件进行完整的评估。

自评估可由发起方实施或委托风险评估服务技术支持方实施。由发起方实施的评估可以降低实施的费用、提高相关人员的安全意识，但可能由于缺乏风险评估的专业技能，其结果不够深入准确；同时，受到组织内部各种因素的影响，其评估结果的客观性易受影响。委托风险评估服务技术支持方实施的评估，过程比较规范、评估结果的客观性比较好，可信程度较高；但由于受到行业知识技能及业务了解的限制，对评估对象的了解，尤其是在业务方面的特殊要求存在一定的局限。由于引入风险评估服务技术支持方本身就是一个风险因素，因此，对其背景与资质、评估过程与结果的保密要求等方面应进行控制。

此外，为保证风险评估的实施，与评估对象相连的相关方也应配合，以防止给其他方的使用带来困难或引入新的风险。

B.2 检查评估

检查评估是指评估对象上级管理部门组织的或国家有关职能部门开展的风险评估。

检查评估可依据本文件的要求，实施完整的风险评估过程。检查评估也可在自评估实施的基础上，对关键环节或重点内容实施抽样评估，包括以下内容（但不限于）：

a） 自评估队伍及技术人员审查；
b） 自评估方法的检查；
c） 自评估过程控制与文档记录检查；
d） 自评估资产列表审查；
e） 自评估威胁列表审查；
f） 自评估脆弱性列表审查；
g） 现有安全措施有效性检查；
h） 自评估结果审查与采取相应措施的跟踪检查；
i） 自评估技术技能限制未完成项目的检查评估；
j） 上级关注或要求的关键环节和重点内容的检查评估；
k） 软硬件维护制度及实施管理的检查；
l） 突发事件应对措施的检查。

检查评估也可委托风险评估服务技术支持方实施，但评估结果仅对检查评估的发起单位负责。由于检查评估代表了主管机关，涉及评估对象也往往较多，因此，要对实施检查评估机构的资质进行严格管理。

附 录 C
（资料性）
风险评估的工具

C.1 概述

风险评估工具是风险评估的辅助手段，是保证风险评估结果可信度的一个重要因素。风险评估工具的使用不但在一定程度上解决了手动评估的局限性，最主要的是它能够将专家知识进行集中，使专家的经验知识被广泛地应用。

根据在风险评估过程中的主要任务和作用原理的不同,风险评估的工具可以分成风险评估与管理工具、系统基础平台风险评估工具、风险评估辅助工具三类。风险评估与管理工具是一套集成了风险评估各类知识和判据的管理信息系统，以规范风险评估的过程和操作方法；或者是用于收集评估所需要的数据和资料，基于专家经验，对输入输出进行模型分析。系统基础平台风险评估工具主要用于对信息系统的主要部件（如操作系统、数据库系统、网络设备等）的脆弱性进行分析，或实施基于脆弱性的攻击。风险评估辅助工具则实现对数据的采集、现状分析和趋势分析等单项功能，为风险评估各要素的赋值、定级提供依据。

C.2 风险评估与管理工具

风险评估与管理工具大部分是基于某种标准方法或某组织自行开发的评估方法,可以有效地通过输入数据来分析风险，给出对风险的评价并推荐控制风险的安全措施。

风险评估与管理工具通常建立在一定的模型或算法之上，风险由业务重要性、资产重要性、所面临的威胁以及威胁所利用的脆弱性来确定；也有的通过建立专家系统，利用专家经验进行分析，给出专家结论。这种评估工具需要不断进行知识库的扩充。

此类工具实现了对风险评估全过程的实施和管理，包括：评估对象基本信息获取、业务信息获取、资产信息获取、脆弱性识别与管理、威胁识别、风险计算、评估过程与评估结果管理等功能。评估的方式可 以通过问卷的方式，也可以通过结构化的推理过程，建立模型、输入相关信息，得出评估结论。通常这类 工具在对风险进行评估后都会有针对性地提出风险控制措施。

根据实现方法的不同，风险评估与管理工具可以分为三类。

a） 基于信息安全标准的风险评估与管理工具。目前,市面上存在多种不同的风险分析标准或指南，不同的风险分析方法侧重点不同。以这些标准或指南的内容为基础，分别开发相应的评估工具，完成遵循标准或指南的风险评估过程。

b） 基于知识的风险评估与管理工具。基于知识的风险评估与管理工具并不仅仅遵循某个单一的标准或指南，而是将各种风险分析方法进行综合，并结合实践经验，形成风险评估知识库，以此为基础完成综合评估。它还涉及来自类似组织的最佳实践，主要通过多种途径采集相关信息，识别组织的风险和当前的安全措施；与特定的标准或最佳实践进行比较，从中找出不符合的地方；按照标准或最佳实践的推荐选择安全措施以控制风险。

c） 基于模型的风险评估与管理工具。基于标准或基于知识的风险评估与管理工具，都使用了定性分析方法或定量分析方法，或者将定性与定量相结合。定性分析方法是目前广泛采用的方法，需要凭借评估方的知识、经验和直觉，或者业界的标准和实践，为风险的各个要素定级。定性分析法操作相对容易，但也可能因为评估方经验和直觉的偏差而使分析结果失准。定量分析则对构成风险的各个要素和潜在损失水平赋予数值或货币金额，通过对度量风险的所有要素进行赋值，建立综合评价的数学模型，从而完成风险的量化计算。定量分析方法准确，但前 期建立系统风险模型较困难。定性与定量结合分析方法就是将风险要素的赋值和计算，根据需要分别采取定性和定量的方法完成。

基于模型的风险评估与管理工具是在对系统各组成部分、安全要素充分研究的基础上，对典型系统的资产、威胁、脆弱性建立量化或半量化的模型，根据采集信息的输入，得到评价的结果。

C.3 系统基础平台风险评估工具

系统基础平台风险评估工具包括脆弱性扫描工具、渗透性测试工具、代码审计工具、移动应用安全测试工具、工控安全测试工具、机房检测工具等。

脆弱性扫描工具又称为安全扫描器、漏洞扫描仪等，主要用于识别网络、操作系统、数据库系统的脆弱性。通常情况下，这些工具能够发现软件和硬件中已知的脆弱性，以决定系统是否易受已知攻击的影响。脆弱性扫描工具是目前应用最广泛的风险评估工具，主要完成操作系统、数据库系统、网络协议、网络服务等的安全脆弱性检测功能，目前常见的脆弱性扫描工具有以下几种类型：

a） 基于网络的扫描器：在网络中运行，能够检测如防火墙错误配置或连接到网络上的易受攻击的网络服务器的关键漏洞；

b） 基于主机的扫描器：发现主机的操作系统、特殊服务和配置的细节，发现潜在的用户行为风险，如密码强度不够，也可实施对文件系统的检查；

c） 基于平台的扫描器：能够发现平台存在的脆弱性，平台包括云平台、大数据平台等；

d） 分布式网络扫描器：由远程扫描代理、对这些代理的即插即用更新机制、中心管理点三部分构成，用于企业级网络的脆弱性评估，分布和位于不同的位置、城市甚至不同的国家；

e） 数据库脆弱性扫描器：对数据库的授权、认证和完整性进行详细的分析，也可以识别数据库系统中潜在的脆弱性。

渗透性测试工具是根据脆弱性扫描工具扫描的结果进行模拟攻击测试，判断被非法访问者利用的可能性。这类工具通常包括黑客工具、脚本文件。渗透性测试的目的是检测已发现的脆弱性是否真正会给系统或网络带来影响。通常渗透性工具与脆弱性扫描工具一起使用，并可能会对被评估系统的运行带来一定影响。

代码审计工具是通过对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议。

App 安全测试工具是通过对 App 的代码、会话、数据、通信等进行安全测试，以发现 App 中存在的脆弱性的工具。

工控安全测试工具是对工业控制系统的网络和应用进行安全性测试，以发现工业控制系统中存在的脆弱性的工具。

C.4 风险评估辅助工具

科学的风险评估需要大量的实践和经验数据的支持，这些数据的积累是风险评估科学性的基础。风险评估过程中，可以利用一些辅助性的工具和方法来采集数据，帮助完成现状分析和趋势判断。

a） 国家漏洞库、专业机构发布的漏洞与威胁统计数据。

b） 检查列表和基线检查工具：检查列表是基于特定标准或基线建立的，对特定系统进行审查的项目条款。通过检查列表，操作者可以快速定位系统目前的安全状况与基线要求之间的差距，该检查工作可以通过基线检查工具实现。

c） 网络入侵检测系统：全流量威胁检测系统、基于日志的失陷检测工具和入侵检测系统等通过部署检测引擎，收集、处理整个网络中的通信信息，以获取可能对网络或主机造成危害的入侵攻 击事件；帮助检测各种攻击试探和误操作；同时也可以作为一个警报器，提醒管理员发生的安全状况。

d） 态势感知系统：态势感知系统通过综合分析网络安全要素，评估安全状况，预测其发展趋势，以可视化的方式展现给用户，并给出相应的报表和应对措施；它的相应报表可以作为安全现状数 据，并用于分析威胁情况。

e）安全审计工具：用于记录网络行为，分析系统或网络安全现状；它的审计记录可以作为风险评估中的安全现状数据，并可用于判断评估对象威胁信息的来源。

f） 拓扑发现工具：通过接入点接入被评估网络，完成被评估网络中的资产发现功能，并提供网络资产的相关信息，包括操作系统版本、型号等。拓扑发现工具主要是自动完成网络硬件设备的 识别、发现功能。

g） 资产信息收集系统：通过提供调查表形式，完成被评估信息系统数据、管理、人员等资产信息的收集功能，了解到组织的主要业务、重要资产、威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况。此类系统主要采取电子调查表形式，需要被评估系统管理人员参与填写，并自动完成资产信息获取。

h） 机房检测工具：对机房环境进行检测的一类工具，用以发现当前机房的情况，具体包括温度检测、湿度检测等。

i） 其他：如用于评估过程参考的评估指标库、知识库、漏洞库、算法库、模型库等。

附 录 D
（资料性）
资产识别

D.1 业务重要性赋值调整表

业务重要性赋值调整见表 D.1。

表 D.1 业务重要性赋值调整表

赋值	标识	定义
5	很高	业务重要性为 4，紧密关联业务的重要性为 5，该业务重要性调整为 5
4	高	业金重要性为 3，紧密关联业务的重要性为 4 以上（含），该业务重要性调整为 4
3	中等	业务重要性为 2，紧密关联业务的重要性为 3 以上（含），该业务重要性调整为 3
2	低	业务重要性为 1，紧密关联业务的重要性为 2 以上（含），该业务重要性调整为 2

D.2 资产保密性赋值方法

根据资产在保密性上的不同要求，将其分为 5 个不同的等级，分别对应资产在保密性上应达成的不同程度或者保密性缺失时对资产造成的影响。表 D.2 提供了一种保密性赋值的参考。

表 D.2 资产保密性赋值表

赋值	标识	定义
5	很高	资产的保密性要求非常高，一旦丢失或泄露会对资产造成重大的或无法接受的影响
4	高	资产的保密性要求较高，一旦丢失或泄露会对资产造成较大影响
3	中等	资产的保密性要求中等，一旦丢失或泄露会对资产造成影响
2	低	资产的保密性要求较低，一旦丢失或泄露会对资产造成轻微影响
1	很低	资产的保密性要求非常低，一旦丢失或泄露会对资产造成的影响可以忽略

D.3 资产完整性赋值方法

根据资产在完整性上的不同要求，将其分为 5 个不同的等级，分别对应资产在完整性上应达成的不同程度或者完整性缺失时对资产造成的影响。表 D.3 提供了一种完整性赋值的参考。

表 D.3 资产完整性赋值表

赋值	标识	定义
5	很高	资产的完整性要求非常高，未经授权的修改或破坏会对资产造成重大的或无法接受的影响
4	高	资产的完整性要求较高，未经授权的修改或破坏会对资产造成较大影响
3	中等	资产的完整性要求中等，未经授权的修改或破坏会对资产造成影响
2	低	资产的完整性要求较低，未经授权的修改或破坏会对资产造成轻微影响
1	很低	资产的完整性要求非常低，未经授权的修改或破坏对资产造成的影响可以忽略

D.4 资产可用性赋值方法

根据资产在可用性上的不同要求，将其分为 5 个不同的等级，分别对应资产在可用性上应达成的不同程度或者可用性缺失时对资产造成的影响。表 D.4 提供了一种可用性赋值的参考。

表 D.4 资产可用性赋值表

赋值	标识	定义
5	很高	资产的可用性要求非常高，合法使用者对资产的可用度达到年度 99.9%以上，或系统不准许中断
4	高	资产的可用性要求较高，合法使用者对资产的可用度达到每天 90%以上，或系统允许中断时间小于 10 min
3	中等	资产的可用性要求中等，合法使用者对资产的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30 min
2	低	资产的可用性要求较低，合法使用者对资产的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60 min
1	很低	资产的可用性要求非常低，合法使用者对资产的可用度在正常工作时间低于 25%

D.5 系统资产业务承载性赋值方法

根据系统资产对所承载业务的影响不同，将其分为 5 个不同的等级，分别对应系统资产在业务承载性上应达成的不同程度或者资产安全属性被破坏时对业务的影响程度。表 D.5 提供了一种系统资产业务承载性赋值的参考。

表 D.5 系统资产业务承载性赋值表

等级	标识	描述
5	很高	资产对于某种业务的影响非常大，其安全属性破坏后可能对业务造成非常严重的损失
4	高	资产对于某种业务的影响比较大，其安全属性破坏后可能对业务造成比较严重的损失
3	中等	资产对于某种业务的影响一般，其安全属性破坏后可能对业务造成中等程度的损失
2	低	资产对于某种业务的影响较低，其安全属性破坏后可能对业务造成较低的损失
1	很低	资产对于某种业务的影响较低，其安全属性破坏后对业务造成很小的损失，甚至忽略不计

附 录 E
（资料性）
威胁识别

E.1 威胁来源分类

威胁来源分类见表 E.1。

表 E.1 威胁来源列表

来源	描述
环境	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
意外	非人为因素导致的软件、硬件、数据、通信线路等方面的故障，或者依赖的第三方平台或者信息系统等方面的故障
人为	人为因素导致资产的保密性、完整性和可用性遭到破坏

E.2 威胁种类

威胁种类见表 E.2。

表 E.2 威胁种类列表

种类	描述
物理损害	对业务实施或系统运行产生影响的物理损害
自然灾害	自然界中所发生的异常现象，且对业务开展或者系统运行会造成危害的现象和事件
信息损害	对系统或资产中的信息产生破坏、篡改、丢失、盗取等行为
技术失效	信息系统所依赖的软硬件设备不可用
未授权行为	超出权限设置或授权进行操作或者使用的行为
功能损害	造成业务或系统运行的部分功能不可用或者损害
供应链失效	业务或系统所依赖的供应商、接口等不可用

E.3 威胁动机分类

威胁动机分类见表 E.3。

表 E.3 威胁动机分类表

分类	动机
恶意	挑战、叛乱、地位、金钱利益、信息销毁、信息非法泄露、未授权的数据更改、勒索、摧毁、非法利用、复仇、政治利益、间谍、获取竞争优势等
非恶意	好奇心、自负、无意的错误和遗漏（例如，数据输入错误、编程错误）等

E.4 特定威胁行为能力赋值

特定威胁行为能力赋值见表 E.4。

表 E.4 特定威胁行为能力赋值表

赋值	标识	描述
3	高	恶意动力高，可调动资源多；严重自然灾害
2	中	恶意动力高，可调动资源少；恶意动力低，可调动资源多；非恶意或意外，可调动资源多；较严重自然灾害
1	低	恶意动力低，可调动资源少；非恶意或意外；一般自然灾害

E.5 威胁行为、种类、来源对应

威胁行为、种类、来源对应见表 E.5。

表 E.5 威胁行为、种类、来源对应表

种类	威胁行为	威胁来源
物理损害	火灾、水灾、污染	环境、人为、意外
	重大事故、设备或介质损害、灰尘、腐蚀、冻结、静电、灰尘、潮湿、温度、鼠蚁虫害	环境、人为、意外
	电磁辐射、热辐射、电磁脉冲	环境、人为、意外
自然灾害	地震、火山、洪水、气象灾害	环境
信息损害	对阻止干扰信号的拦截、远程侦探、窃听、设备偷窃、回收或废弃介质的检索、硬件篡改、位置探测、信息被窃取、个人隐私被入侵、社会工程事件、邮件勒索、数据篡改、恶意代码	人为
	内部信息泄露、外部信息泄露、来自不可信源数据、软件篡改	人为、意外
技术失效	空调或供水系统故障	人为、意外
	电力供应失去	环境、人为、意外
	外部网络故障	人为、意外
	设备失效、设备故障、软件故障	意外
	信息系统饱和、信息系统可维护性破坏	人为、意外
未授权行为	未授权的设备使用、软件的伪造复制、数据损坏、数据的非法处理	人为
	假冒或盗版软件使用	人为、意外
功能损害	操作失误、维护错误	意外
	网络攻击、权限伪造、行为否认（抵赖）、媒体负面报道	人为
	权限滥用	人为、意外
	人员可用性破坏	环境、人为、意外
供应链失效	供应商失效	人为、意外
	第三方运维问题、第三方平台故障、第三方接口故障	人为、意外

E.6 威胁种类、资产、威胁行为关联分析示例

威胁种类、资产、威胁行为关联分析示例见表 E.6。

表 E.6 威胁种类、资产、威胁行为关联分析示例表

资产	种类	威胁行为
硬件设备，如服务器、网络 设备	软硬件故障	设备硬件故障，如服务器损害、网络设备故障
机房	物理环境影响	机房遭受地震，火灾等
信息系统	网络攻击	非授权访问网络资源、非授权访问系统资源等
外包服务人员	人暴失控	滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等
组织形象	网络攻击	媒体负面报道

E.7 威胁频率的赋值方法

威胁频率赋值方法见表 E.7。

表 E.7 威胁频率赋值表

等级	标识	
5	很高	出现的频率很高；或在大多数情况下几乎不可避免；或可以证实经常发生过
4	高	出现的频率较高；或在大多数情况下很有可能会发生；或可以证实多次发生过
3	中等	出现的频率中等；或在某种情况下可能会发生；或被证实曾经发生过
2	低	出现的频率较小；或一般不太可能发生；或没有被证实发生过
1	很低	威胁几乎不可能发生；仅可能在非常罕见和例外的情况下发生

参 考 文 献

[1] 国务院办公厅政府信息公开目录
[2] 国家自然资源与空间地理数据库
[3] 江苏省公共数据管理办法
[4] 浙江省人民政府办公厅关于印发浙江省公共数据开放与安全管理暂行办法实施方案的通知