风险评估

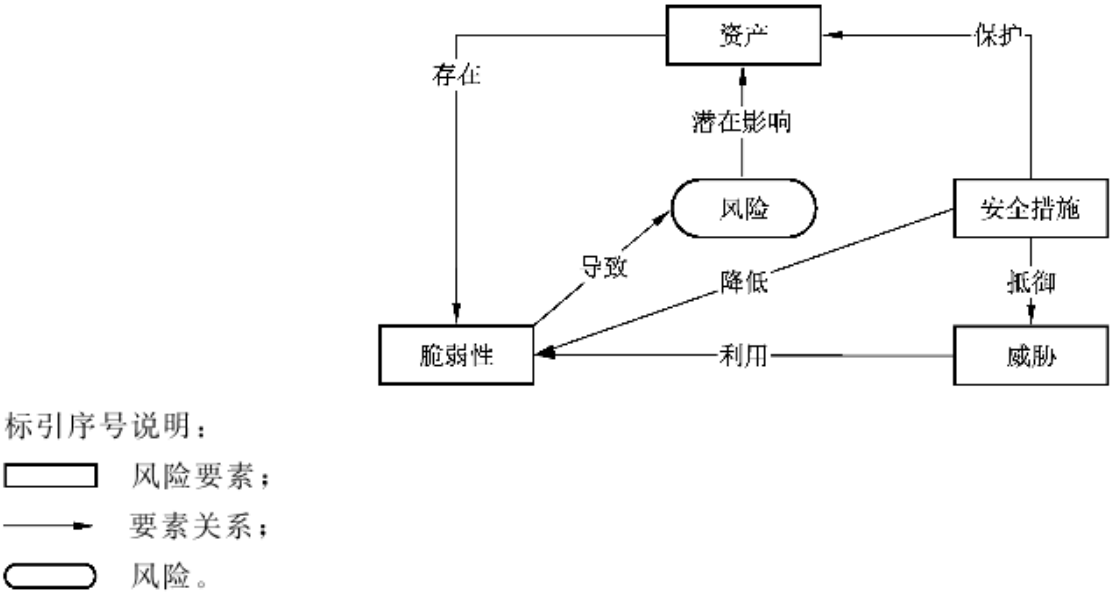
01 风险评估基础

1.1 风险评估概念

信息安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解信息安全风险，将风险控制在可接受的水平，最大限度地保障信息安全提供科学依据。

1.2 风险要素关系

风险评估中各要素的关系如下图所示：



基本要素的定义：

a）资产：对组织有价值的信息或资源，是安全策略保护的对象。

b）威胁：可能导致对系统或组织危害等不希望事故的潜在起因。

c）脆弱性：可能被威胁所利用的资产或若干资产的薄弱环节。

d）风险：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。

e）安全措施：保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

开展风险评估时，基本要素之间的关系如下：

a）风险要素的核心是资产，而资产存在脆弱性；

b）安全措施的实施通过降低资产脆弱性被利用难易程度，抵御外部威胁，以实现对资产的保护；

c）威胁总是要利用资产存在的脆弱性才能导致风险；

d）风险转化成安全事件后，会对资产的运行状态产生影响。

风险分析时，应综合考虑资产、脆弱性、威胁和安全措施等基本因素。

1.3 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；

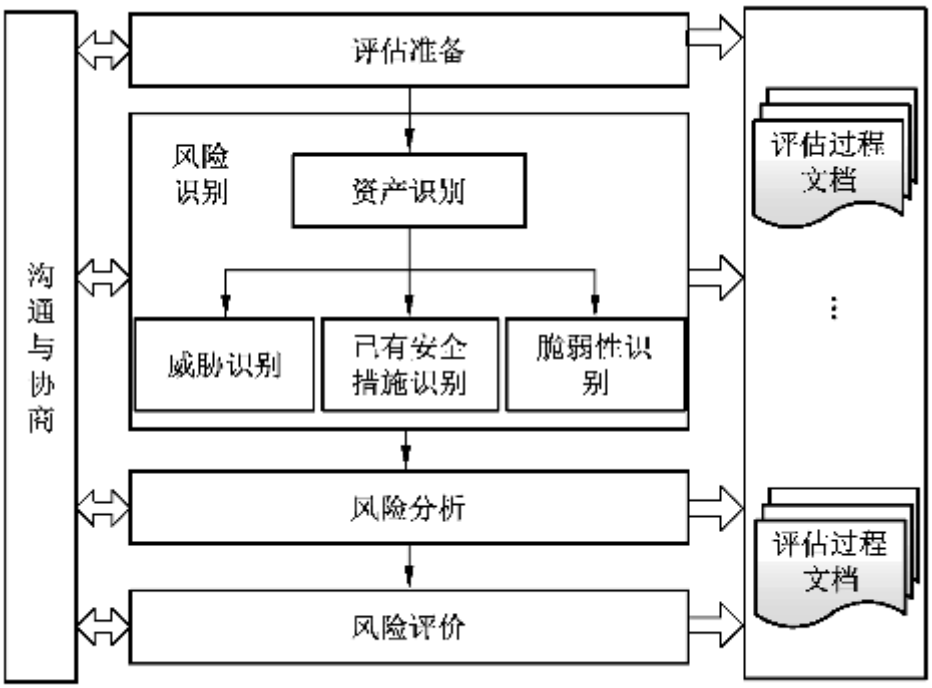
f）根据影响程度和资产价值，确定安全事件发生后对评估对象造成的损失；

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。

1.4 风险评估流程

风险评估的实施流程如下图所示：



根据流程中的各项工作内容，一般将风险评估实施划分为评估准备、风险识别、风险分析与风险评价四个阶段：

1、评估准备，此阶段应包括：

a）确定风险评估的目标

b）确定风险评估的对象、范围和边界

c）组建评估团队

d）开展前期调研

e）确定评估依据

f）建立风险评价准则

g）制定评估方案

组织应形成完整的风险评估实施方案，并获得组织最高管理者的支持和批准。

2、风险识别，此阶段应包括：

a）资产识别

b）威胁识别

c）已有安全措施识别

d）脆弱性识别

3、风险分析，此阶段依据识别的结果计算得到风险值。

4、风险评价，此阶段依据风险评价准则确定风险等级。

风险评估的结果能够为风险处理提供决策支撑，风险处理是指对风险进行处理的一系列活动,如接受风险、规避风险、转移风险、降低风险等。

1.5 风险评估工作形式

风险评估的基本工作形式是自评估与检查评估。

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，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。

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。检查评估可依据国标文件的要求，实施完整的风险评估过程；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。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。

信息安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充。

1.6 信息系统生命周期内的风险评估

信息系统生命周期一般包括信息系统的规划、设计、实施、交付、运维和废弃六个阶段，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：
1、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；
2、设计阶段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；
3、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；
4、交付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；
5、运行维护阶段风险评估的目的是了解和控制运维过程中的安全风险，是一种较为全面的风险评估。评估内容包括真实运行的资产、威胁、脆弱性等各方面；
6、废弃阶段风险评估应重点围绕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。

在上述各阶段中，运行维护阶段的风险评估工作最为全面，也是在实际工作中最常遇到的情况。因此，本次课程内容基于运行维护阶段的风险评估进行展开，简单理解就是对已建成并投入使用的信息系统进行风险评估。

02 风险评估实施

2.1 准备阶段

准备阶段工作流程如下图所示：

2.1.1 确定评估目标及范围

目标：前面提到过，由于信息系统生命周期各阶段中风险评估实施的内容、对象、安全需求均不同，因此组织应首先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，并以此来明确风险评估目标。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，识别现有信息系统及管理上的不足，以及可能造成的风险大小。
范围：风险评估范围可以是组织全部的信息及与信息处理相关的各类资产、管理机构，也可以是某个独立的信息系统、关键业务流程等。

2.1.2 组建团队

评估机构成员角色：项目组长、安全技术评估人员、安全管理评估人员；
被评估组织成员角色：项目组长、信息安全管理人员、项目协调人、业务人员、运维人员、开发人员；
风险评估领导小组：被评估组织信息技术部门领导、相关业务部门领导等；
专家组：对于大型复杂的风险评估项目，应考虑在项目期间聘请相关领域的专家对风险评估项目的关键阶段进行工作指导。

2.1.3 系统调研（重点工作）

系统调研是确定被评估对象的过程，为风险评估依据和方法的选择、评估内容的实施奠定基础。
调研内容应包括：
a）系统安全保护等级；
b）主要的业务功能和要求；
c）网络结构与网络环境，包括内部连接和外部连接；
d）系统边界，包括业务逻辑边界、网络及设备载体边界、物理环境边界、组织管理权限边界等；
e）主要的硬件、软件；
f）数据和信息；
g）系统和数据的敏感性；
h）支持和使用系统的人员；
i）信息安全管理组织建设和人员配备情况；
j）信息安全管理制度；
k）法律法规及服务合同；
l）其他。
系统调研可以采取问卷调查、现场面谈相结合的方式进行。

2.1.4 确定评估依据及方法

根据风险评估目标以及系统调研结果，确定评估依据和评估方法。评估依据应包括：
a）适用的法律、法规；
b）现行国际标准、国家标准、行业标准；
c）行业主管机关的业务系统的要求和制度；
d）与信息系统安全保护等级相应的基本要求；
e）被评估组织的安全要求；

f）系统本身的实时性或性能要求等。
根据评估依据，应考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险计算方法，并依据业务实施对系统安全运行的需求，确定相关的判断依据，使之能够与组织环境和安全要求相适应。

2.1.5 制定评估方案

风险评估方案是评估工作实施活动总体计划，用于管理评估工作的开展，使评估各阶段工作可控，并作为评估项目验收的主要依据之一。风险评估方案应得到被评估组织的确认和认可。风险评估方案的内容应包括：
a）风险评估工作框架：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;如有必要还应包括风险评估领导小组和专家组组建介绍等；
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）风险规避：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。

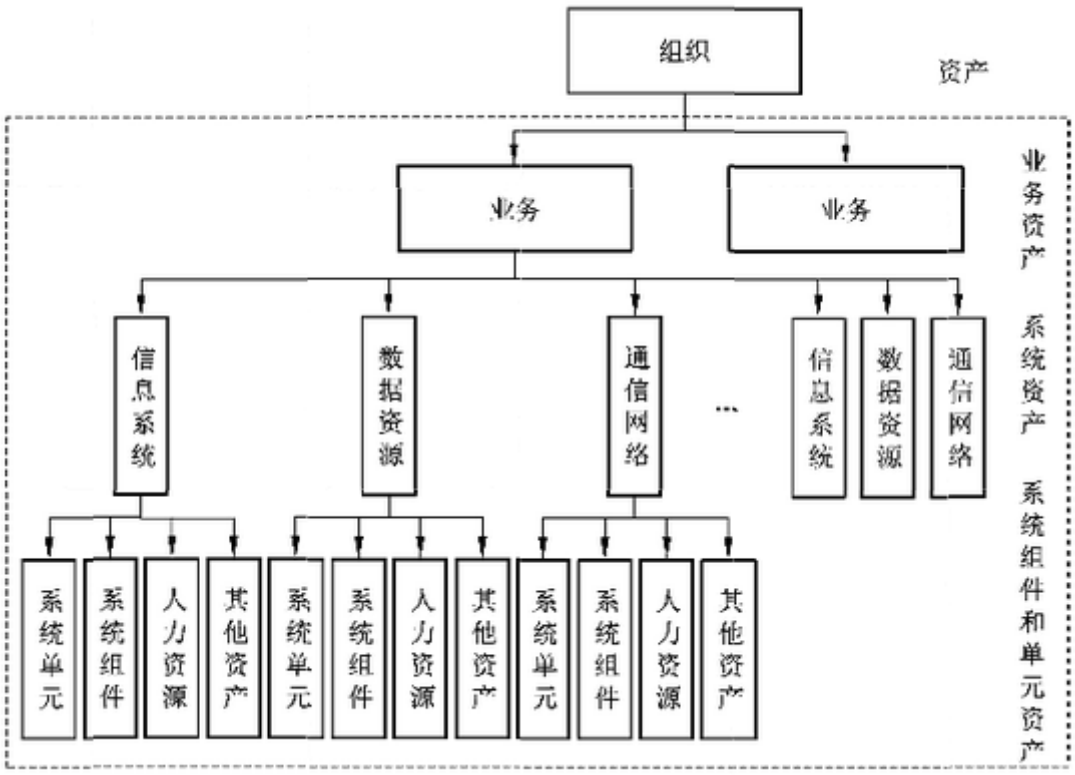
2.1.6 获得高层支持

上述所有内容确定后，应形成较为完整的风险评估实施方案，得到组织最高管理者的支持、批准；对管理层和技术人员进行传达，在组织范围内就风险评估相关内容进行培训，以明确有关人员在风险评估中的任务。

2.2 识别阶段

2.2.1 资产识别

资产识别是风险评估的核心环节。在《GBT 20984-2007 信息安全技术 信息安全风险评估规范》将资产划分为硬件、软件、数据、服务、人员以及其他六大类，而在2022版中，资产识别重新做了定义：按照层次可划分为业务资产、系统资产、系统组件和单元资产，如下图所示。



2.2.1.1 业务识别

业务是实现组织发展规划的具体活动，业务识别内容包括业务的属性、定位、完整性和关联性识别。

识别内容	示例
属性	业务功能、业务对象、业务流程、业务范围、覆盖地域等
定位	发展规划中的业务属性和职能定位、与发展规划目标的契合度、业务布局中的位置和作用、竞争关系中竞争力强弱等
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
关联性	关联类别：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依赖，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） 关联程度：如果被评估业务遭受重大损害，将会造成关联业务无法正常开展，此类关联为紧密关联，其他为非紧密关联

业务识别数据应来自熟悉组织业务结构的业务人员或管理人员，既可通过访谈、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。
根据业务的重要程度进行等级划分，并对其重要性进行赋值：

赋值	标识	定义
5	很高	业务在规划中极其重要，在发展规划中的业务属性及职能定位层面具有重大影响，在规划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
4	高	业务在规划中较为重要，在发展规划中的业务属性及职能定位层面具有较大影响，在规划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
3	中等	业务在规划中具有一定重要性，在发展规划中的业务属性及职能定位层面具有一定影响，在规划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
2	低	业务在规划中具有一定重要性，在发展规划中的业务属性及职能定位层面影响较低，在规划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
1	很低	业务在规划中具有一定重要性，在发展规划中的业务属性及职能定位层面影响很低，在规划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

业务的关联性会对业务的重要性造成影响，若被评估业务与高于其重要性赋值的业务具有紧密关联关系，则该业务重要性赋值应在原赋值基础上进行赋值调整。

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	业务重要性为 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

2.2.1.2 系统资产识别

系统资产识别包括资产分类和业务承载性识别两个方面。

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）

系统资产价值赋值

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。
注意：这里提到的“综合计算”，在国标文件中并未给出明确的计算方式，需要组织综合考虑业务情况和特点，自行确定（可参考2.2.1.4）。

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

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

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

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%

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

综上，系统资产价值主要还是依据资产的保密性、完整性和可用性进行计算和赋值，业务承载性、业务重要性可作为辅助参考因素。

2.2.1.3 系统组件和单元资产识别

系统组件和单元资产应分类识别，分类包括系统单元、系统组件、人力资源和其他资产。

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 PaaS 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

系统组件和单元资产价值赋值

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。
注意：
（1）这里提到的“综合计算”，同样没给出计算方式；
（2）资产保密性、完整性、可用性赋值方法参照2.2.1.2。

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

2.2.1.4 资产赋值

资产赋值方法有两种：
1、根据信息系统所承载的业务对不同安全属性的依赖程度，选择资产保密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果；
2、根据资产保密性、完整性和可用性的不同等级对其赋值进行加权计算得到资产的最终赋值结果，加权方法可根据组织的业务特点确定。

2.2.2 威胁识别

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。

2.2.2.1 威胁来源识别

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：

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

威胁主体依据环境和人为进行区分，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，人为的分为国家、组织团体和个人。

2.2.2.2 威胁种类识别

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。

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

2.2.2.3 威胁动机识别

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。

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

威胁来源、种类、动机识别完成后，接下来进行威胁赋值工作。

2.2.2.4 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。

等级	标识	威胁赋值描述
5	很高	根据威胁的行为能力、频率和时机，综合评价等级为很高
4	高	根据威胁的行为能力、频率和时机，综合评价等级为高
3	中等	根据威胁的行为能力、频率和时机，综合评价等级为中
2	低	根据威胁的行为能力、频率和时机，综合评价等级为低
1	很低	根据威胁的行为能力、频率和时机，综合评价等级为很低

从上面这段话我们可以提取出来：

（1）威胁赋值的3个相关要素：威胁的行为能力、频率、时机；

（2）威胁赋值综合计算的方法并未直接给出，需要组织综合考虑业务情况和特点，自行确定。

1、威胁能力赋值

威胁能力是指威胁来源完成对组织业务、资产产生影响的活动所具备的资源和综合素质。组织及业务所处的地域和环境决定了威胁的来源、种类、动机，进而决定了威胁的能力；应对威胁能力进行等级划分，级别越高表示威胁能力越强。此外，威胁动机对威胁能力有调整作用。

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

从上面这张表可以知道，想对威胁的行为能力进行赋值的话，需要从威胁来源（涉及恶意动力和可调动资源）、威胁种类（自然灾害及等级）、威胁动机（恶意或者非恶意）进行综合评估。

威胁的种类和资产决定了威胁的行为，威胁行为、种类、来源的对应关系参考如下：

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

资产、威胁种类、威胁行为具备关联关系，参考如下：

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	人员安全失控	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

2.2.1资产识别的过程中，资产因素已经具备；2.2.2.1~2.2.2.3过程中，每个资产所面临的威胁来源、种类和动机也识别完成。至此，资产及其面临的威胁来源、种类、动机全部确定下来，可以进行威胁能力赋值。

举例：张三在工作中心存不满，故意引起火灾，导致机房受损。
资产：运维人员、机房
威胁来源：人为（恶意动力高、可调动资源多）、火灾（严重灾害）
威胁种类：人员安全失控、物理损害
威胁动机：恶意
推导出威胁能力赋值：3-高

2、威胁频率赋值

威胁出现的频率应进行等级化处理，不同等级分别代表威胁出现频率的高低。等级数值越大，威胁出现的频率越高。此外，威胁时机对威胁频率有调整作用。

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。

下面这张图取自GBT 20984-2007，GBT 20984-2022只是把数字内容去掉了，描述部分完全一致。

等级	标识	定　　义
5	很高	出现的频率很高(或≥1 次/周)；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≥1 次/月)；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＞1 次/半年)；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

3、威胁时机赋值

风险评估国标文件中规定威胁时机可分为普通时期、特殊时期和自然规律，但是未给出明确的赋值定义，仅说明了威胁时机对威胁频率有调整作用，暂作参考使用。
举例：国家重大活动期间（特殊时期）遭受国外攻击的可能性更高，此时在给各项威胁参数赋值时要适当提升。

综上，威胁的行为能力、频率、时机赋值全部完成，根据组织自定义的综合计算方法得出最终的威胁赋值。

2.2.3 已有安全措施识别

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，保护性安全措施可以减少安全事件发生后对组织或系统造成的影响。

举例：
预防性安全措施：消防演练
保护性安全措施：配备灭火器

在识别脆弱性的同时，应对已采取的安全措施的有效性进行确认：
有效的安全措施：继续保持，以避免不必要的工作和费用，防止安全措施的重复实施；
不适当的安全措施：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。

2.2.4 脆弱性识别

脆弱性是资产本身存在的，如果脆弱性没有对应的威胁，则无需实施控制措施，但应注意并监视它们是否发生变化；相反，如果威胁没有对应的脆弱性，也不会导致风险。即，威胁总是要利用资产的脆弱性才可能造成风险。不过要注意，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。

资产的脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分（举例：系统有0day，被打了才知道存在该漏洞）。因此，脆弱性识别时的数据应来自于资产的所有者、使用者，以及相关业务领域和软硬件方面的专业人员等。脆弱性可从技术和管理两个方面进行审视，技术脆弱性涉及IT环境的物理层、网络层、系统层、应用层等各个层面的安全问题或隐患，管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

脆弱性识别可以以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的脆弱性，并对脆弱性的严重程度进行评估；也可以从物理、网络、系统、应用等层次进行识别，然后与资产、威胁对应起来。脆弱性识别的依据可以是国际或国家安全标准，也可以是行业规范、应用流程的安全要求。对应用在不同环境中的相同的脆弱性，其影响程度是不同的，评估方应从组织安全策略的角度考虑，判断资产的脆弱性被利用难易程度及其影响程度。

对不同的识别对象，其脆弱性识别的具体要求应参照相应的技术或管理标准实施，参考如下：

类型	识别对象	识别方面
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别
	系统软件	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别

2.2.4.1 脆弱性赋值

脆弱性赋值包括两部分，一部分是脆弱性被利用难易程度赋值，一部分是影响程度赋值。

1、脆弱性被利用难易程度赋值

脆弱性被利用难易程度赋值需要综合考虑已有安全措施的作用。一般来说，安全措施的使用将降低系统技术或管理上脆弱性被利用难易程度，但安全措施确认并不需要和脆弱性识别过程那样具体到每个资产、组件的脆弱性，而是一类具体措施的集合。
依据脆弱性和已有安全措施识别结果，得出脆弱性被利用难易程度，并进行等级化处理，不同的等级代表脆弱性被利用难易程度高低。等级数值越大，脆弱性越容易被利用。（举例：MS17-010漏洞的修复方法）

等级	标识	定义
5	很高	实施了控制措施后，脆弱性仍然很容易被利用
4	高	实施了控制措施后，脆弱性较容易被利用
3	中等	实施了控制措施后，脆弱性被利用难易程度一般
2	低	实施了控制措施后，脆弱性难被利用
1	很低	实施了控制措施后，脆弱性基本不可能被利用

2、影响程度赋值

影响程度赋值是指脆弱性被威胁利用导致安全事件发生后对资产价值所造成影响的轻重程度分析并赋值的过程。识别和分析资产可能受到的影响时，需要考虑受影响资产的层面。可从业务层面、系统层面、系统组件和单元三个层面进行分析。
影响程度赋值需要综合考虑安全事件对资产保密性、完整性和可用性的影响。影响程度赋值采用等级划分处理方式，不同的等级分别代表对资产影响的高低。等级数值越大，影响程度越高。

等级	标识	定义
5	很高	如果脆弱性被威胁利用，将对资产造成特别重大损害
4	高	如果脆弱性被威胁利用，将对资产造成重大损害
3	中等	如果脆弱性被威胁利用，将对资产造成一般损害
2	低	如果脆弱性被威胁利用，将对资产造成较小损害
1	很低	如果脆弱性被威胁利用，将对资产造成的损害可以忽略

2.3 风险分析阶段

风险分析是在完成了资产识别、威胁识别、脆弱性识别，以及已有安全措施确认后，采用适当的方法与工具确定每个资产面临威胁利用脆弱性导致安全事件发生的可能性，对业务相关的资产、威胁、脆弱性及其各项属性做关联分析，综合进行风险分析和计算：

1、根据威胁的能力和频率，以及脆弱性被利用难易程度，计算安全事件发生的可能性；

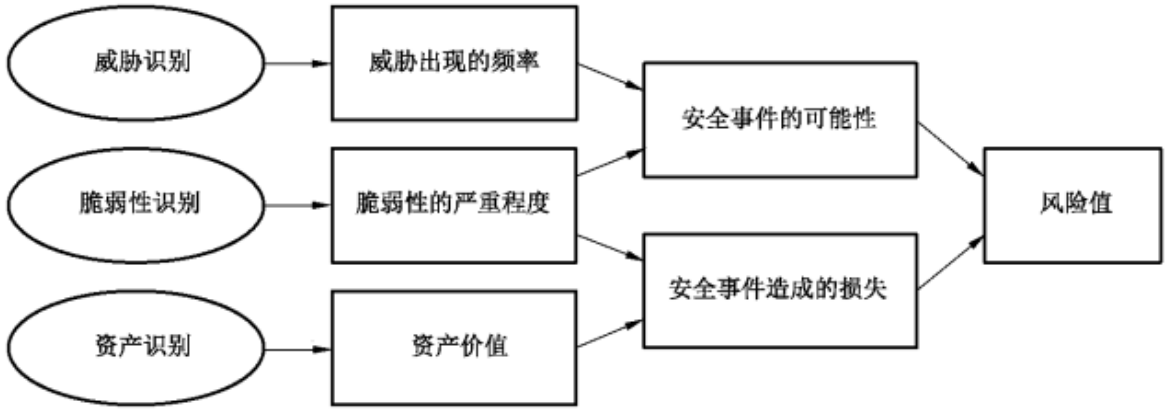
2、根据安全事件造成的影响程度和资产价值，计算安全事件发生后对评估对象造成的损失；

3、根据安全事件发生的可能性以及安全事件发生后造成的损失，计算系统资产面临的风险值；

4、根据业务所涵盖的系统资产风险值综合计算得出业务风险值。

2.3.1 风险分析模型

构建风险分析模型是将资产、威胁、脆弱性三个基本要素及每个要素相关属性进行关联，建立各要素之间的相互作用机制关系。



首先，通过威胁与脆弱性进行关联，哪些威胁可以利用哪些脆弱性引发安全事件，并分析安全事件发生的可能性；

其次，通过资产与脆弱性进行关联，哪些资产存在脆弱性，一旦安全事件发生，造成的损失有多大；

最后，根据安全事件发生的可能性和造成的损失，计算出每个资产的风险值。

2.3.2 风险计算方法

风险计算方法一般分为定性计算方法和定量计算方法两大类：

a）定性计算方法是将风险的各要素资产、威胁、脆弱性等的相关属性进行量化（或等级化）赋值，然后选用具体的计算方法（如相乘法或矩阵法）进行风险计算；

b）定量计算方法是通过将资产价值和风险等量化为财务价值的方式来进行计算的一种方法。由于定量计算法需要等量化财务价值，在实际操作中往往难以实现。

由于定量计算方法在实际工作中可操作性较差，一般风险计算多采用定性计算方法。风险的定性计算方法实质反应的是组织或信息系统面临风险大小的准确排序，确定风险的性质（无关紧要、可接受、待观察、不可接受等），而不是风险计算值本身的准确性。

分析方法	定性分析	定量分析
优点	1、不需要大量复杂计算 2、分析过程可清楚各类角色成员的意见 3、能提供一般风险领域和指标	1、通过量化赋值更易于自动化评估 2、能够对风险管理性能进行追踪能够提供可信的成本/收益分析 3、衡量标准客观并且可验证 4、能够明确衡量一年内可能造成的损失
缺点	1、评估方法及结果相对主观 2、无法为成本/收益分析建立货币价值 3、使用主观衡量难易跟踪风险管理目标	1、计算较为复杂，需有一定专业知识 2、需要做大量基础性工作，需收集与环境相关的详细信息 3、结果存在一定的不确定性，元素的赋值过程非完全客观

本节内容重点在于了解有哪些计算方法，不具体介绍如何计算。因为在实际测评过程中，测评方通常会提供计算表格模板，将前期识别到的资产、威胁和脆弱性的赋值输入其中，便会自动计算出风险值。

2.4 风险评价阶段

2.4.1 系统资产风险评价

根据风险评价准则对系统资产风险计算结果进行等级处理。

等级	标识	描述
5	很高	风险发生的可能性很高，对系统资产产生很高的影响
4	高	风险发生的可能性很高，对系统资产产生中等及高影响 风险发生的可能性高，对系统资产产生高及以上影响 风险发生的可能性中，对系统资产产生很高影响
3	中等	风险发生的可能性很高，对系统资产产生低及以下影响 风险发生的可能性高，对系统资产产生中及以下影响 风险发生的可能性中，对系统资产产生高、中、低影响
2	低	风险发生的可能性中，对系统资产产生很低影响 风险发生的可能性低，对系统资产产生低及以下影响 风险发生的可能性很低，对系统资产产生中、低影响
1	很低	风险发生的可能性很低，发生后对系统资产几乎无影响

2.4.2 业务风险评价

根据风险评价准则对业务风险计算结果进行等级处理，在进行业务风险评价时，可从社会影响和组织影响两个层面进行分析。社会影响涵盖国家安全，社会秩序，公共利益，公民、法人和其他组织的合法权益等方面；组织影响涵盖职能履行、业务开展、触犯国家法律法规、财产损失等方面。

等级	标识	描述
5	很高	社会影响： a） 对国家安全、社会秩序和公共利益造成影响； b） 对公民、法人和其他组织的合法权益造成严重影响 组织影响： a） 导致职能无法履行或业务无法开展； b） 触犯国家法律法规； c） 造成非常严重的财产损失
4	高	社会影响： 对公民、法人和其他组织的合法权益造成较大影响 组织影响： a） 导致职能履行或业务开展受到严重影响； b） 造成严重的财产损失
3	中等	社会影响： 对公民、法人和其他组织的合法权益造成影响 组织影响： a） 导致职能履行或业务开展受到影响； b） 造成较大的财产损失
2	低	组织影响： a） 导致职能履行或业务开展受到较小影响； b） 造成一定的财产损失
1	很低	组织影响： 造成较少的财产损失

风险等级处理的目的是对不同风险进行直观比较，以便在接下来的风险处理阶段对不同风险采取对应的处理措施。

2.5 风险处理阶段

2.5.1 风险处理原则

风险处理依据风险评估结果，针对风险分析和评价阶段输出的风险评估报告进行风险处理。
风险处理的基本原则是适度接受风险，根据组织可接受的处置成本将残余安全风险控制在可以接受的范围内。

注意：依据国家、行业主管部门发布的信息安全建设要求进行的风险处理，应严格执行相关规定。如依据等级保护相关要求实施的安全风险加固工作，应满足等级保护相应等级的安全技术和管理要求；对于因不能够满足该等级安全要求产生的风险则不能够适用适度接受风险的原则。对于有着行业主管部门特殊安全要求的风险处理工作，同样不适用该原则。

2.5.2 风险处理方式

风险处理方式一般包括接受、消减、转移、规避、不适用：
a）接受：风险值不高或者处理的代价高于风险引起的损失，组织决定接受该风险/残余风险；
b）消减：通过适当的控制措施降低风险发生的可能性；
c）转移：通过购买保险、外包等方法把风险转移到外部机构；
d）规避：决定不进行引起风险的活动，从而避免风险；
e）不适用：该项风险对于组织不适用。

安全整改是风险处理中常用的风险消减方法，风险评估需提出安全整改建议。
安全整改建议需根据安全风险的严重程度、加固措施实施的难易程度、降低风险的时间紧迫程度、所投入的人员力量及资金成本等因素综合考虑。
a）对于非常严重、需立即降低且加固措施易于实施的安全风险，建议被评估组织立即采取安全整改措

施；
b）对于非常严重、需立即降低，但加固措施不便于实施的安全风险，建议被评估组织立即制定安全整改实施方案，尽快实施安全整改；整改前应对相关安全隐患进行严密监控，并作好应急预案；
c）对于比较严重、需降低且加固措施不易于实施的安全风险，建议被评估组织制定限期实施的整改方案；整改前应对相关安全隐患进行监控。

2.5.3 残余风险处理

残余风险处理是风险评估活动的延续，是被评估组织按照安全整改建议全部或部分实施整改工作后，对仍然存在的安全风险进行识别、控制和管理的活动。
对于已完成安全加固措施的信息系统，为确保安全措施的有效性，可进行残余风险评估，评估流程及内容可做有针对性的剪裁。残余风险评估的目的是对信息系统仍存在的残余风险进行识别、控制和管理，如某些风险在完成了适当的安全措施后，残余风险的结果仍处于不可接受的风险范围内，应考虑进一步增强相应的安全措施。