第七章

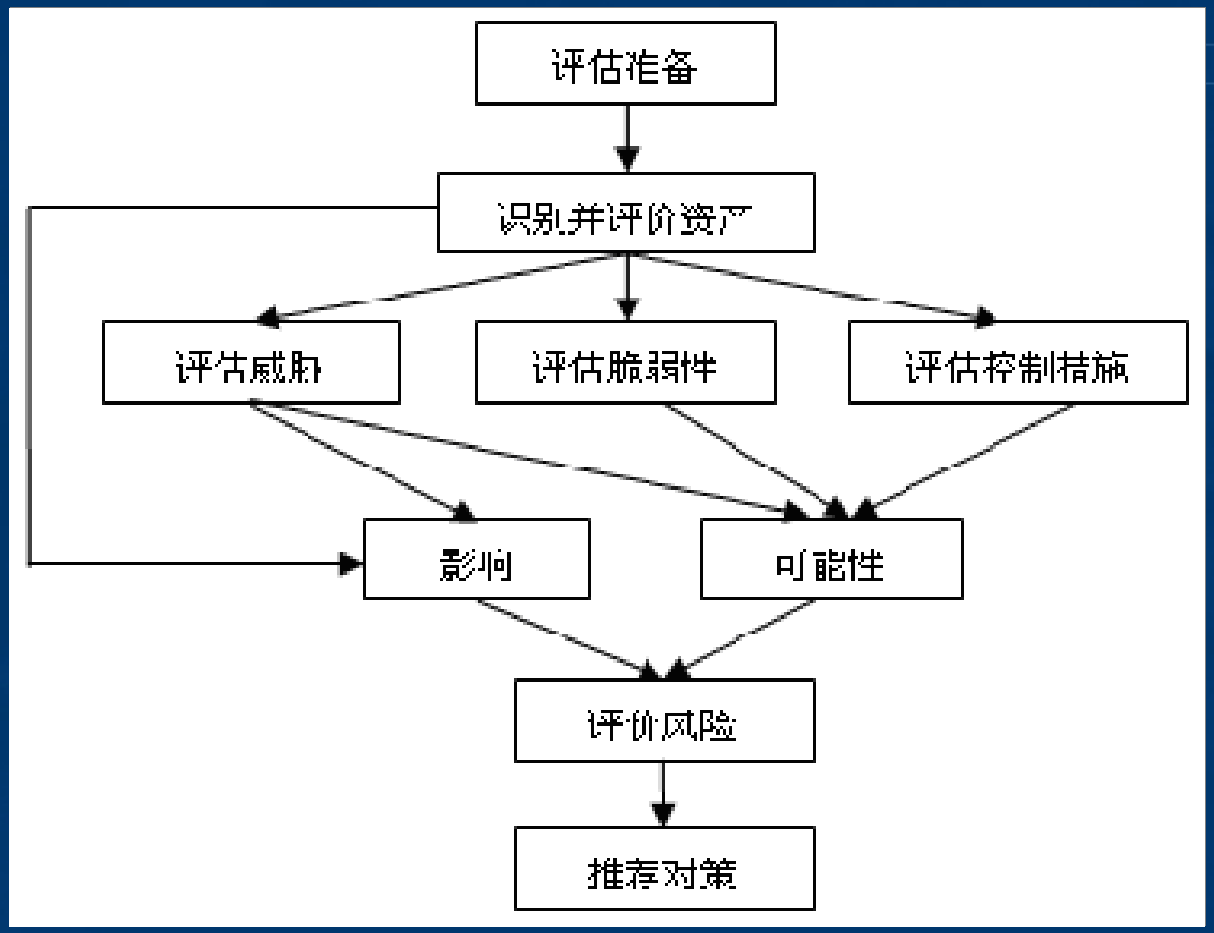
信息安全风险评估的基本过程

信息安全风险评估是对信息在产生、存储、传播等过程中其机密性、完整性、可用性遭到破坏的可能性及由此产生的后果所做的估计或估价，是组织拟定信息安全需求的过程。

7.1　信息安全风险评估的过程

根据GB/T 20984—2023《信息安全技术 信息安全风险评估规范》，同步参照ISO/IEC TR 13335-3、NIST SP800-30等原则，风险评估过程都会涉及到下列阶段：辨认要评估的资产，拟定资产的威胁、脆弱点及有关问题，评价风险，推荐对策。

信息安全风险评估完整的过程如图7-1所示



7.2 评估准备

信息安全风险评估的准备，是实施风险评估的前提。为了确保评估过程的可控性以及评估成果的客观性，在信息安全风险评估实施前应进行充分的准备和计划，信息安全风险评估的准备活动涉及：

(1) 拟定信息安全风险评估的目的；

(2) 拟定信息安全风险评估的范围；

(3) 组建合适的评估管理与实施团队；

(4) 进行系统调研；

(5) 拟定信息安全风险评估根据和措施；

(6) 制定信息安全风险评估方案；

(7) 取得最高管理者对信息安全风险评估工作的支持。

7.2.1　拟定信息安全风险评估的目的

在信息安全风险评估准备阶段应明确风险评估的目的，为信息安全风险评估的过程提供导向。信息安全需求是一种组织为确保其业务正常、有效运转而必须到达的信息安全要求，经过分析组织必须符合的有关法律法规、组织在业务流程中对信息安全等的保密性、完整性、可用性等方面的需求，来拟定信息安全风险评估的目的。

7.2.2　拟定信息安全风险评估的范围

既定的信息安全风险评估可能只针对组织全部资产的一种子集，评估范围必须明确。

描述范围最主要的是对于评估边界的描述。评估的范围可能是单个系统或者是多种关联的系统。

比很好的措施是按照物理边界和逻辑边界来描述某次风险评估的范围。

7.2.3　组建合适的评估管理与实施团队

在评估的准备阶段，评估组织应成立专门的评估团队，详细执行组织的信息安全风险评估。团队组员应涉及评估单位领导、信息安全风险评估教授、技术教授，还应该涉及管理层、业务部门、人力资源、IT系统和来自顾客的代表。

7.2.4 进行系统调研

系统调研是拟定被评估对象的过程。风险评估团队应进行充分的系统调研，为信息安全风险评估根据和措施的选择、评估内容的实施奠定基础。调研内容至少应涉及：

(1) 业务战略及管理制度；
(2) 主要的业务功能和要求；
(3) 网络构造与网络环境，涉及内部连接和外部连接；
(4) 系统边界；
(5) 主要的硬件、软件；
(6) 数据和信息；
(7) 系统和数据的敏感性；
(8) 支持和使用系统的人员。

7.2.5　拟定信息安全风险评估根据和措施

信息安全风险评估根据涉及既有国际或国家有关信息安全原则、组织的行业主管机关的业务系统的要求和制度、组织的信息系统互联单位的安全要求、组织的信息系统本身的实时性或性能要求等。

根据信息安全评估风险根据，并综合考虑信息安全风险评估的目的、范围、时间、效果、评估人员素质等原因，选择详细的风险计算措施，并根据组织业务实施对系统安全运营的需求，拟定有关的评估判断根据，使之能够与组织环境和安全要求相适应。

7.2.6　制定信息安全风险评估方案

信息安全风险评估方案的内容一般涉及：

⑴ 团队组织：涉及评估团队组员、组织构造、角色、责任等内容。

⑵ 工作计划：信息安全风险评估各阶段的工作计划，涉及工作内容、工作形式、工作成果等内容。

⑶ 时间进度安排：项目实施的时间进度安排。

7.2.7　取得最高管理者对信息安全风险评估工作的支持

信息安全风险评估需要有关的财力和人力的支持，管理层必须以明示的方式表白对评估活动的支持，对资源调配作出承诺，并对信息安全风险评估小组赋予足够的权利，信息安全风险评估活动才干顺利进行。

7.3 辨认并评价资产

7.3.1 辨认资产

在信息安全风险评估的过程中，应清楚地辨认其全部的资产，不能漏掉，划入风险评估范围和边界内的每一项资产都应该被确认和评估。

- 资产辨认活动中，可能会用到工具有以下几种。
- 1．资产管理工具
- 2．主动探测工具
- 3．手工登记表格

7.3.2　资产分类

资产的分类并没有严格的原则，在实际工作中，详细的资产分类措施能够根据详细的评估对象和要求，由评估者灵活把握，表7-2列出了一种根据资产的体现形式的资产分类措施。

表7-2 一种基于体现形式的资产分类措施

分类	示例
数据	• 保存在信息媒介上的多种数据资料，涉及源代码、数据库数据、系统文档、运营管理规程、计划、报告、顾客手册、各类纸质的文档等
软件	• 系统软件：操作系统、数据库管理系统、语言包、开发系统等 • 应用软件：办公软件、数据库软件、各类工具软件等 • 源程序：多种共享源代码、自行或合作开发的多种代码等
硬件	• 网络设备：路由器、网关、互换机等 • 计算机设备：大型机、小型机、服务器、工作站、台式计算机、便携式算机等 • 存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等

7.3.3.1　定性分析

定性风险评估一般将资产按其对于业务的主要性进行赋值，成果是资产的主要度列表。资产的主要度一般定义为“高”、“中”、“低”等级别，或直接用数字1～3表达。组织能够按照自己的实际情况选择3个级别、5个级别等，表7-3给出了5级分法的资产主要性等级划分表。

表7-3 资产等级及含义描述

等级	标识	定义
5	很高	• 非常主要，其安全属性破坏后可能对组织造成非常严重的损失
4	高	• 主要，其安全属性破坏后可能对组织造成比较严重的损失
3	中	• 比较主要，其安全属性破坏后可能对组织造成中档程度的损失
2	低	• 不太主要，其安全属性破坏后可能对组织造成较低的损失
1	很低	• 不主要，其安全属性破坏后对组织造成很小的损失，甚至忽视不计

信息安全风险评估中资产的价值不是以资产的经济价值来衡量，而是以资产的保密性、完整性和可用性三个安全属性为基础进行衡量。资产在保密性、完整性和可用性三个属性上的要求不同，则资产的最终价值也不同，表7-4、表7-5、表7-6分别给出了资产的保密性、完整性和可用性的赋值表。

表7-4　资产保密性赋值表

赋值	标识	定义
5	很高	• 涉及组织最主要的秘密，关系将来发展的前途命运，对组织的根本利益有着决定性的影响，假如泄漏会造成劫难性的损害
4	高	• 涉及组织的主要秘密，其泄露会使组织的安全和利益遭受严重损害
3	• 中档	• 涉及组织的一般性秘密，其泄露会使组织的安全和利益受到损害
2	低	• 仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成损害
1	很低	• 可对社会公开的信息，公用的信息处理设备和系统资源等

表7-5 资产完整性赋值表

赋值	标识	定义
5	很高	• 完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补
4	高	• 完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补
3	• 中档	• 完整性价值中档，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但能够弥补
2	低	• 完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，能够忍受，对业务冲击轻微，轻易弥补
1	很低	• 完整性价值非常低，未经授权的修改或破坏对

表7-6 资产可用性赋值表

赋值	标识	定义
5	很高	• 可用性价值非常高，正当使用者对信息及信息系统的可用度到达年度99.9%以上，或系统不允许中断
4	高	• 可用性价值较高，正当使用者对信息及信息系统的可用度到达每天90%以上，或系统允许中断时间不不小于10min
3	• 中档	• 可用性价值中档，正当使用者对信息及信息系统的可用度在正常工作时间到达70%以上，或系统允许中断时间不不小于30min
2	低	• 可用性价值较低，正当使用者对信息及信息系统的可用度在正常工作时间到达25%以上，或系统允许中断时间不不小于60min

7.3.3.2　定量分析

定量风险评估对资产进行赋值，应该拟定资产的货币价值，但这个价值并不是资产的购置价值或帐面价值，而是相对价值。在定义相对价值时，需要考虑：

1．信息资产因为受损而对商务造成的直接损失；

2．信息资产恢复到正常状态所付出的代价，涉及检测、控制、修复时的人力和物力；

3．信息资产受损对其他部门的业务造成的影响；

4．组织在公众形象和声誉上的损失；

5．因为商务受损造成竞争优势降级而引起的间接损失；

6．其他损失，例如保险费用的增长。

7.3.4 输出成果

在资产划分的基础上，再进行资产的统计、汇总，形成完备的《资产及评价报告》。

7.4 辨认并评估威胁

7.4.1 威胁辨认

辨认并评价资产后，组织应该辨认每项（类）资产可能面临的威胁，辨认威胁时，应该根据资产目前所处的环境条件和此前的统计情况来判断。一项资产可能面临多种威胁，一种威胁也可能对不同的资产造成影响。

威胁辨认活动中，可能会用到工具有下列几种：

1. IDS采样分析
2. 日志分析
3. 人员访谈

7.4.2　威胁分类

在对威胁进行分类前，首先要考虑威胁的起源。

表7-8 威胁起源列表

• 起源	描述
• 环境原因	• 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
	• 不满的或有预谋的内部人员对信

对威胁进行分类的方式有多种多样，针对上表威胁起源，能够根据其体现形式将威胁分为下列种类。

1. 软硬件故障
2. 物理环境影响
3. 无作为或操作失误
4. 管理不到位
5. 恶意代码
6. 越权或滥用
7. 网络攻击
8. 物理攻击
9. 泄密
10. 篡改
11. 抵赖

7.4.3　威胁赋值

辨认资产面临的威胁后，还应该评估威胁出现的频率。威胁出现的频率是衡量威胁严重程度的主要原因。

表7-10 威胁赋值表

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防止；或能够证明经常发生过
4	高	• 出现的频率较高（或≥1次/月）；在大多数情况下很有可能会发生；或能够证明屡次发生过
3	中	• 出现的频率中档（或＞1次/六个月）；或在某种情况下可能会发生；或被证明曾经发生过
2	低	• 出现的频率较小；或一般不太可能发生；或没有被证明发生过
1	很低	• 威胁几乎不可能发生；仅可能在非常罕见

7.4.4 输出成果

表7-11 威胁列表达例1

威胁编号	威胁类别	威胁赋值	描述

表7-12 威胁列表达例2

威胁编号	威胁类别	• 详细威胁	威胁描述	• 威胁起源	后果	威胁赋值	• 受影响的设备名称（IP）