风险评估 信息安全风险评估资质

产品名称	风险评估 信息安全风险评估资质
公司名称	腾创实验室（广州）有限公司
价格	.00/件
规格参数	品牌:腾创实验室 测试类型:信息安全风险评估 报告范围:全国
公司地址	广州市黄埔区彩频路9号502-1、502-2房（注册地址）
联系电话	020-32206063 13825019240

产品详情

风险评估是指，在风险事件发生之前或之后（但还没有结束），该事件给人们的生活、生命、财产等各个方面造成的影响和损失的可能性进行量化评估的工作。即，风险评估就是量化测评某一事件或事物带来的影响或损失的可能程度。

信息安全风险评估，腾创实验室（广州）有限公司（简称“ 腾创实验室 ”）依据《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）、《国家网络与信息安全协调小组关于开展信息安全风险评估工作的意见》（国信办[2006]5号）、GB/T 20984-2022《信息安全技术 信息安全风险评估方法》等标准规范，进行信息系统安全保障能力级的符合性测评。风险分析中要涉及资产、威胁、脆弱性三个基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。

信息安全服务资质是对信息系统安全服务的提供者的技术、资源、法律、管理等方面的资质和能力，以及其稳定性、可靠性进行评估，并依据公开的标准和程序，对其安全服务保障能力进行认证的过程。

第1：资质级别

信息安全服务资质级别分为一级、二级、三级，其中一级最高，三级最低。资质级别是衡量服务提供者服务能力的尺度。

第2：认证类别

1.安全集成服务资质

2.安全运维服务资质

3.风险评估服务资质

4.应急服务资质

5.软件安全开发服务资质

6.信息系统灾难备份与恢复服务资质

7.工业控制安全服务资质

8.网络安全审计服务资质认证

信息安全风险评估的概念涉及资产、威胁、脆弱性和风险4个主要因素。

根据GB/T 20984-2022《信息安全技术 信息安全风险评估方法》，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。

1.资产识别

资产识别是风险评估的核心环节。资产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。因此资产识别应从三个层次进行识别。

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

3.脆弱性识别

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。相反，如果威胁没有对应的脆弱性,也不会导致风险。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。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。

4.风险分析

组织应在风险识别基础上开展风险分析,风险分析应: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;a)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;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:d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。

信息安全风险评估是信息安全保障的基础性工作和重要环节，贯穿于网络和信息系统建设运行的全过程。通过对信息系统提供风险评估服务，系统地分析网络与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安全整改措施，防范和消除信息安全风险，或将风险控制在可接受的水平，为网络和信息安全保障提供科学依据。