

# 信息安全风险评估，保护企业网络系统安全

产品名称	信息安全风险评估，保护企业网络系统安全
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 测试报告类型:软件安全评估报告 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

随着互联网的迅猛发展，企业在日常运营中越来越依赖于网络系统。然而，随之而来的是各种各样的信息安全威胁，如数据泄露、黑客攻击和恶意软件等。

信息安全风险评估是保护信息系统和网络安全的重要手段。

信息安全风险评估的定义：

信息安全风险评估是通过对企业信息系统的全面检测和分析，识别出潜在的安全风险并评估其可能的影响程度和概率，为企业制定有效的信息安全保护措施提供依据。它能够帮助企业全面了解自身的信息系统安全风险情况，及时发现并弥补各类漏洞和缺陷，提高信息系统的安全性和可靠性。

信息安全风险评估系统的设计是针对组织开展信息安全风险评估的过程。这个过程包括对信息系统中的安全风险识别、信息收集、评估和报告等。

腾创实验室（广州）有限公司拥有丰富的信息安全风险评估实战经验，可以帮助企业在信息安全运营过程中，实现合法合规的同时，又能制定相应的控制目标和实施相应的控制措施，协助企业持续改进信息安全管理体系，有效实现组织整体经营战略。

风险评估的实施过程如下：

- 1.评估前准备。在风险评估实施前，需要对以下工作进行确定：确定风险评估的目标、确定风险评估的范围、组建风险评估团队、进行系统调研、确定评估依据和方法、制定评估计划和评估方案、获得管理者对工作的支持。
- 2.资产识别。资产识别过程分为资产分类和资产评价两个阶段。资产分类是将单位的信息资产分为实物资产、软件资产、数据资产、人员资产、服务资产和无形资产六类资产进行识别;资产评价是对资产的三个安全属性保密性、可用性及完整性分别等级评价及赋值，经综合评定后，得出资产的价值。
- 3.威胁识别。威胁识别主要工作是评估者需要从每项识别出的资产出发，找到可能遭受的威胁。识别威胁之后，还需要确定威胁发生的可能性。
- 4.脆弱性识别。评估者需要从每项识别出的资产和对应的威胁出发，找到可能被利用的脆弱性。识别脆弱性之后，还需要确定弱点可被利用的严重性。
- 5.已有安全措施确认。在识别脆弱性的同时，评估人员将对已采取的安全措施的有效性进行确认，评估其是否真正地降低了系统的脆弱性，抵御了威胁。

6.风险分析。风险评估中完成资产赋值、威胁评估、脆弱性评估后，在考虑已有安全措施的情况下，利用恰当的方法与工具确定威胁利用资产脆弱性发生安全事件的可能性，并结合资产的安全属性受到破坏后的影响得出信息资产的风险。