云南网络安全风险报告评估机构

产品名称	云南网络安全风险报告评估机构
公司名称	河南世耀诚实业集团有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:文案定制 服务方向:专业领域
公司地址	南阳市卧龙区工业路华龙广告二楼
联系电话	13140513661 18338218580

产品详情

什么是风险评估：对各方面风险进行辨识和分析的过程，是依据国际/国家有关信息安全技术标准，评估信息系统的脆弱性、面临的威胁以及脆弱性被威胁源利用的可能性，和利用后对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性所产生的实际负
面影响，并以此识别信息系统的安全风险的过程。

为什么需要风险评估

分析信息系统及其所依托的网络信息系统的安全状况，全面了解和掌握该系统面临的信息安全威胁和风险，明确采取何种有效措施，降低威胁事件发生的可能性或者其所造成的影响，减少信息系统的脆弱性，从而将风险降低到可接受的水平；同时，为后期安全规划方案的提出提供原始依据，并做为今后其他工作的参考。

充分反映当前的安全现状；

提供信息安全防御机制的建议；

很好的同等级保护相结合；

对安全决策提供支撑和依据；

为今后网络安全建设提供参考；

提高员工的安全意识；

风险评估服务内容

信息安全保障本质上是风险管理的工作，信息安全风险和事件不可能完全避免，关键在于如何控制、化解和规避风险。信息安全保障是高技术的对抗，有别于传统安全，呈现扩散速度快、难控制等特点，必须采取符合信息安全规律的科学方法和手段来保障信息安全。信息安全风险评估是科学方法之一。

通过长期积累的各类信息安全服务和评估经验，结合国际和国内各类信息安全标准，总结出一套信息安全风险评估的方法和流程，以客户行业特点为基础，通过规范的流程和标准的方法，充分对全网进行深入的评估，确定客户信息安全现状和安全风险。

在风险评估服务中，参照安全模型，根据自己的工程实践，建立了自己的风险评估模型，描述如下：

在的风险评估模型中，主要包含信息资产，弱点/脆弱性、威胁和风险四个要素。每个要素有各自的属性，信息资产的属性是资产价值，弱点的属性是弱点被威胁利用后对资产带来的影响的严重程度，威胁的属性是威胁发生的可能性，风险的属性是风险发生的路径。

风险评估服务流程

服务阶段

阶段工作内容

阶段成果输出

阶段1:

准备阶段

项目准备

对信息系统风险评估项目目标、范围、项目交付文件、项目实施方案、工作方式、评估成果提交形式讨论确定。

项目启动

启动信息系统风险评估工作。 《风险评估实施方案》

阶段2:

识别阶段

资产识别

对被评估信息系统的关键资产进行识别，并合理分类；

威胁识别

识别被评估信息系统的关键资产所面临的威胁源，及其威胁所常采用的威胁方法，对资产所产生的影响。

脆弱性识别

将针对每一项需要保护的信息资产，找出每一种威胁所能利用的脆弱性，将从安全管理脆弱性以及技术脆弱性两个方面进行脆弱性检查。

安全措施识别

识别被评估信息系统的有效对抗风险的防护措施。《安全现状调查报告》

阶段3:

分析阶段

资产分析

分析被评估信息系统及其关键资产在遭受泄密、中断、损害等破坏时对系统所承载的业务系统所产生的影响，并进行赋值量化。

威胁分析

分析被评估信息系统及其关键资产将面临哪一方面的威胁及其所采用的威胁方法，并进行赋值量化。

脆弱性分析

分析被评估信息系统及其关键资产所存在的管理脆弱性和技术脆弱性，并进行赋值量化。

综合风险分析

分析被评估信息系统及其关键资产将面临哪一方面的威胁及其所采用的威胁方法,利用了系统的何种脆弱性，对哪一类资产，产生了什么样的影响，并描述采取何种对策来防范威胁，减少脆弱性，同时将风险量化。《资产评估报告》

《威胁评估报告》

《脆弱性评估报告》

《风险评估综合报告》

阶段4:

规划验收

阶段

风险规划

明确组织的安全需求，制定安全规划对风险进行处理。

成果汇报

提交评估成果系列报告同时为客户讲解评估过程及结果，对每个安全问题提出解决建议或整改措施；

项目验收

客户达成安全成果共识，项目验收。

《风险控制规划》

风险评估安全服务收益

通过对信息业务系统风险评估，充分全面了解业务系统安全现状，其结果与业务系统特点紧密结合，通过对信息系统关键资产所存在脆弱性及其所面临的威胁的量化分析，而终以全面、准确、量化的分析结果呈现其面临的各种风险，并提供针对性的安全风险控制方法，消除安全风险，提高业务系统运转效率。

评估结果记录

安全评估报告

安全评估报告

评估成果汇总

严重安全问题及时告知客户

清除检测过程中间测试文件

过程经验总结

评估成果汇报

检测过程

检测深度

检测结果

评估输出报告

评估成果保密

结合评估结果报告和实际信息系统安全情况提供具有针对性的安全解决建议。

风险评估安全服务准则

保密原则

在为信息系统进行风险评估的过程中，将严格遵循保密原则，服务过程中涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

互动原则

在整个信息安全风险评估过程之中，将强调客户的互动参与，不管是从准备阶段，还是识别阶段。每个阶段都能够及时根据客户的要求和实际情况对评估的内容、方式作出相关调整，进而更好的进行风险评估工作。

小范围影响原则

信息安全风险评估工作应尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等）

规范性原则

信息安全风险评估服务的实施必须由专 业的安全评估服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。