甘肃网络安全风险评估编制编写

产品名称	甘肃网络安全风险评估编制编写
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

网络安全风险评估是指从风险管理的角度，运用科学的手段，系统分析网络与信息系统所面临的威胁及其存在的脆弱性。通过开展风险评估工作，企业组织可以对重要信息系统所面临的信息安全风险进行发现识别和定性评估。同时根据评估结果，企业可以更有针对性地进行威胁管控和处置，对企业网络安全建设中的薄弱环节进行优先处理和加固。这样可以更有效的提升企业网络安全防护水平。

安全事件的发生是有概率的，不能只根据安全威胁的发现时间和可能后果，便决定网络安全的投入和安全措施的强度。对于一些被实际利用的概率极低的安全风险，即使其具有比较严重的爆发后果，也不需要不计代价地进行修复处置。企业在开展网络安全风险评估时，必须坚持综合考虑安全事件的后果影响及其可利用性的评价原则。

网络安全风险评估还需要组织确定关键业务目标，并识别对实现这些目标至关重要的信息资产，然后识别可能对这些资产带来不利影响的网络攻击，从而准确了解相关业务所面临的威胁环境。这可以让业务部门和安全团队共同做出优化的处置决定，实施合理的安全控制措施，将整体风险隐患降低到企业能够接受的范围中。

风险评估的关键要素

开展网络安全风险评估涉及到资产、威胁、脆弱性等许多基础性要素，每个要素都有各自的要求和属性。为了保障风险评估工作取得预定的实际效果，企业应该在评估中做好以下方面的工作要素准备：

要素1：确定评估范围

ISO/IEC 27001标准和NIST SP 800-37等主流安全框架。

要素2：识别信息资产

有效开展网络安全风险评估，需要明确知道应该保护的对象是谁，因此，评估团队应该识别并清点风险评估范围内的所有包括软件和硬件在内的信息资产。对业务至关重要的资产不仅是识别和清点的重点，也同样是攻击者的主要目标，所以需要在资产识别的基础上，尽可能做好系统威胁暴露面的管理。通过对信息资产的清点，不仅便于可视化资产和流程之间的连接路径，还可以了解网络的出入点，从而使识别威胁隐患变得更加容易。

要素3：了解威胁利用方法

威胁利用方法是指不法分子可能使用的对组织资产造成损害的策略、技术和方法。为了帮助识别各项信息资产可能存在的威胁隐患，在风险评估中应该使用MITRE ATT&CK之类的威胁知识库，直观地呈现典型攻击的各种阶段和目标，这样有助于确定他们需要的保护类型。

要素4：分析潜在风险

分析潜在风险是为了评估风险场景实际发生的可能性，以及一旦发生后对组织造成的影响。在网络安全风险评估中，风险实际发生的可能性应该取决于威胁和漏洞的可发现性、可利用性和可再现性，而不是取决于历史经验的套用。影响是指威胁利用漏洞的后果对组织造成的危害程度，应在每个场景中评估对机密性、完整性和可用性造成的影响。这一部分的评估在本质上是非常主观的，因此评估者的专业度和经验积累就非常重要。

要素5：确定风险优先级

通过使用风险矩阵（风险级别为“ 可能性乘以影响 ”）可以对每个风险场景进行分类。为了确保企业的网络安全风险程度是可控的，任何高于约定容忍程度的威胁场景都应优先被处理，有三种方法可以做到这一点：第 一是避免，如果风险大于好处，那么立刻停止该项活动可能是正确的行动方案；第二是转移，通过网络保险或将某些业务外包给第三方，与其他方分担部分风险；第三是缓解，部署安全控制措施，降低风险程度。

要素6：记录所有风险

网络安全风险评估是一项重大且持续的工作。随着新威胁层出不穷，新的系统或活动不断引入，安全风险评估需要重复进行。因此，需要在每一次的评估工作中，做好可为未来的评估提供可重复的流程和模板。同时，有必要在风险注册中心记下所有已识别的风险场景。保持定期审查和更新，确保管理层始终了解其网络安全风险的新的信息，主要包括：风险场景、鉴定日期、现有的安全控制、当前风险程度、处理计划、进展状况、残余风险以及风险处置负责人等。