Upon reading the posts and responses by my peers, it is fairly conclusive that despite CVSS being a very well rounded and robust approach at scoring risks and vulnerabilities, it does not fulfil enough criteria’s that give a full detailed input of what actually a risk would be.

A workable risk scoring system or framework must at least provide meaningful and actionable risk information, improve through continuous assessments, and present the overall security posture from a variety of perspectives.

In conclusion, just basing a risk on a vulnerability looks fine if you’re looking at something basic like a penetration testing report; however, other factors such as organizational context, relevancy, placement of the asset within the network hierarchy and other variables must be considered when talking about a risk.

* NIST (2021). NIST Cyber Risk Scoring (CRS) Program Overview. Available from: https://csrc.nist.gov/CSRC/media/Presentations/nist-cyber-risk-scoring-crs-program-overview/images-media/NIST%20Cyber%20Risk%20Scoring%20(CRS)%20-%20Program%20Overview.pdf [Accessed 27 Oct. 2022].