Consensus Building on Risk Ranking. Paper details: Before beginning work on this activity, please review the Microsoft Security Update Guide FAQs Links to an external site.. https://www.microsoft.com/en-us/msrc/faqs-security-update-guide As discussed, to effectively rank risks, we often include input from multiple stakeholders to ensure we get a clear picture of the risk picture regarding the enterprise. Depending on the specific risk items, we may need to work closely with network administrators, policymakers, or technical staff to make a clear determination of the veritable risk for certain areas, as well as the recommended steps required to address it. Citing this, your task is to apply the consensus-building dynamic for risk ranking to a very common procedural workflow that you may be all too familiar with: Patch Tuesday. Part 1: Your task is to determine prioritization based on the provided data and facts about specific patches in relation to known vulnerabilities and security issues. As you more than likely know, Microsoft issues system patches on a regular cadence in an event often referred to as Patch Tuesday. Using this as an example, discuss your organization's approach to reviewing, assessing, and ranking risk efforts as it may apply to patching vulnerable Microsoft systems or applications after updates are released. Please use the following questions as a discussion guide: Describe the organizational approach for reviewing and ranking risk within the organization. How would this construct apply to the regular Patch Tuesday release? Does routine Microsoft patching differ from other patching or vulnerability management activities in general? Please describe the method of incorporating input from stakeholders into a risk prioritization plan. Which key stakeholders, relevant third parties, or various departments are included as part of the process? What specific role(s) do they play in assisting, advising, or supporting the risk ranking activities? Discuss how you incorporate the input(s) from multiple parties into a risk prioritization plan. Part 2: Now assume that you become aware of an immediate release of security updates for critical vulnerabilities that are pertinent to your organization. Would the expedited deployment differ from the Patch Tuesday process? Would different stakeholders be involved in general? Submission instructions: Your initial post should be a minimum of 250 words.