Guidelines and Rubric

1. **Planning and Security**
	1. Recommend the best approach to mitigate the potential **performance and security issues** that you previously identified, and defend your response.
	2. Recommend a **network management tool** to implement into the future network and explain its potential benefit to the organization.
	3. Recommend types of **security devices** that you would implement into the existing network, and explain how the devices would mitigate potential security issues.
	4. Explain the **changes** **that need to be made to existing devices** on the network in order to successfully integrate the security devices into the future network design.
	5. Describe specific **challenges** that the organization might face as it attempts to implement the future network, and recommend ways to mitigate those challenges.
	6. Concisely explain the **overall risk** for the network and the organization of not keeping security services up to standard.

# Rubric

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Planning and Security:** **Performance and** **Security Issues**   | Meets “Proficient” criteria and defense demonstrates keen insight into how to mitigate potential issues that may occur within the network (100%)  | Recommends the best approach to mitigate the previously identified potential performance and security issues and defends response (90%)  | Recommends the best approach to mitigate the previously identified potential performance and security issues, but does not defend response, or defense is cursory or illogical or contains inaccuracies (70%)  | Does not recommend the best approach to mitigate the previously identified potential performance and security issues (0%)  | 6  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Planning and** **Security: Network** **Management Tool**   | Meets “Proficient” criteria and explanation demonstrates keen insight into how the organization would benefit from the recommended network management tool (100%)  | Recommends a network management tool to implement into the future network and explains its potential benefit to the organization (90%)  | Recommends a network management tool to implement into the future network, but does not explain its potential benefit to the organization, or explanation is cursory or illogical or contains inaccuracies (70%)  | Does not recommend a network management tool to implement into the future network (0%)  | 3.6  |
| **Planning and** **Security: Security** **Devices**   | Meets “Proficient” criteria and explanation demonstrates a complex grasp of how the recommended security devices would mitigate potential security issues (100%)  | Recommends types of security devices to implement into the existing network and explains how the devices would mitigate potential security issues (90%)  | Recommends types of security devices to implement into the existing network, but does not explain how the devices would mitigate potential security issues, or explanation is cursory or illogical or contains inaccuracies (70%)  | Does not recommend types of security devices to implement into the existing network (0%)  | 3.6  |
| **Planning and** **Security: Changes to** **Existing Devices**   | Meets “Proficient” criteria and explanation demonstrates a sophisticated awareness of the changes that are required for existing devices (100%)  | Explains the changes that need to be made to existing devices on the network in order to successfully integrate the security devices into the future network design (90%)  | Explains the changes that need to be made to existing devices on the network in order to successfully integrate the security devices into the future network design, but explanation is cursory or illogical or contains inaccuracies (70%)  | Does not explain the changes that need to be made to existing devices on the network (0%)  | 3.6  |
| **Planning and** **Security: Challenges**   | Meets “Proficient” criteria and recommendations demonstrate nuanced understanding of how to plan for the challenges associated with implementing a new network (100%)  | Describes specific challenges that the organization might face as it attempts to implement the future network and recommends ways to mitigate those challenges (90%)  | Describes challenges that the organization might face as it attempts to implement the future network but does not recommend ways to mitigate those challenges, recommendations are inappropriate, or challenges described are not specific (70%)  | Does not describe challenges that the organization might face as it attempts to implement the future network (0%)  | 3.6  |
| **Planning and** **Security: Overall Risk**   | Meets “Proficient” criteria and explanation provides keen insight into the importance of keeping security services up to standard (100%)  | Concisely explains the overall risk for the network and the organization of not keeping security services up to standard (90%)  | Explains the overall risk for the network and the organization of not keeping security services up to standard, but explanation is illogical or contains inaccuracies (70%)  | Does not explain the overall risk for the network and the organization of not keeping security services up to standard (0%)  | 3.6  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Articulation of Response**  | Submission is free of errors related to citations, grammar, spelling, syntax, and organization and is presented in a professional and easy-toread format (100%)  | Submission has no major errors related to citations, grammar, spelling, syntax, or organization (90%)  | Submission has major errors related to citations, grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas (70%)  | Submission has critical errors related to citations, grammar, spelling, syntax, or organization that prevent understanding of ideas (0%)  | 5  |
|  |  |  |  | **Total**  | **100%**  |