Report- Cybersecurity Risk Assessment of AMC

- **Title Page**- This page contains the name of the group, course ID, section number, the name of team members, and the Aggie Honor Code signed/initialed by each team member.
- **Table of Contents Page**
- **Executive Summary**- No more than a page. Contains a summary of your project goals, your assessment of the cybersecurity risks that AMC faces, and your recommendation to minimize those risks
- **Asset Identification**- A brief explanation of your task in this phase of the project and the list of assets identified by your team.
  [NOTE: you will lose points if you do not provide a rationale for including an asset in this list].
- **Vulnerability and Threat Identification**- A brief explanation of your task in this phase of the project. Provide (in table format) the threat statements for each asset. Based on your project guidelines, you should have at least 4 threat statements for each asset, and these statements should include at least two technical vulnerabilities (with CVE IDs) and two non-technical vulnerabilities (due to gaps in administrative and physical controls). Refer to the appropriate appendix for explanation of the vulnerabilities. For each threat statement, refer to the appropriate appendix for related tree analysis. [NOTE: You would lose additional points if the non-technical vulnerabilities identified in this phase are not supported by evidence from the case, i.e. you *assume* these vulnerabilities to exist without any evidence from the case].
- **Cybersecurity Risk Estimation**- A brief explanation of your task in this phase of the project. Provide (in table format) the cybersecurity risk associated with each threat statements for each asset. This section should also contain the scores of Likelihood and Impact for each threat statement. Refer to the appropriate appendix for explanation of these scores.
- **Cyber Security Risk Management Strategy**- Provide cybersecurity risk management strategy for each threat statement. Where the strategy is to mitigate or eliminate risk, provide specific controls that need to be implemented. Where possible (of if information available online) provide the cost of implementing these controls.
- **Appendices- Measurement Scales**
  - **Appendix A**- Provide the Vulnerability-Threat identification tree(s) in this appendix. Also, provide a brief description of the vulnerabilities in this section.
    - **For the technical vulnerabilities-** Provide their CVE ID, a link to the NVD page where information is available for this vulnerability, a brief description of the vulnerability, Exploitability Score, Impact Score, and Vector information (e.g., *Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)*.
    - **For the non-technical vulnerabilities-** Provide evidence from the case that this vulnerability exists, a brief description of the vulnerability, calculated Exploitability Score, calculated Impact Score, and Vector information (e.g., *Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)*. This vector is generated for you when you calculate the base score for the vulnerability. It informs the readers about the values that you chose to calculate the Exploitability and Impact Scores.
  - **Appendix B-** Measurement Scale for scoring Threat Likelihood (in terms of CVSS V3 Exploitability Scores)
  - **Appendix C**-. Estimation of Impact (as a function of Asset Value Scores and/or CVSS V3 Impact Score).
  - **Appendix D**- Cybersecurity Risk Matrix and Risk Management Strategy for various cybersecurity risk values
  - **Appendix E**- Any assumptions made by the project team.
  -
- **References**
- **Glossary-** Provide a brief explanation of terms and abbreviations to explain them to a reader who is not an expert in information systems and/or cybersecurity
- **Team Work-** Provide (in table format) the contribution of each group member to the project

Additional Suggestions

1. Number and label each table and figure.
2. Number the pages.
3. Proofread for grammatical and/or spelling mistakes.
4. Format the report to improve its readability.