## Risk Assessment Report

# IT Department

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| System or Application Information | | | | | | | | | | | | | | | |
| System/App Name: | | | |  | | | | | | Overall Rating: | | |  | | |
| Description: | | |  | | | | |  | | | |  | | | |
| Primary Users: | | | |  | | | Authorizing Official: | | | | |  | | | |
| Reported By: | | | |  | | | Report Date: | | | | |  | | | |
|  |  | | | | | | | |  | | | | |  |
|  |  | | | | | | | |  | | | | |  |
|  |  | | | | | | | |  | | | | |  |
| Risk of Data DisclosureStatus | | | | | | | | | | | | | | |
| Risk No. | | Data Type | | | Present (Yes or No) | Risk (High, Medium, or Low) | | | | | Likelihood (High, Medium, Low) | | | Risk Calculation |
| 1 | | Critical Data | | |  |  | | | | |  | | |  |
| 2 | | Limited-Access Data | | |  |  | | | | |  | | |  |
| Risk of Service DenialStatus | | | | | | | | | | | | | | |
| Risk No. | | Denial Type | | | Possible (Yes or No) | Risk (High, Medium, or Low) | | | | | Likelihood (High, Medium, Low) | | | Risk Calculation |
| 3 | | Degradation | | |  |  | | | | |  | | |  |
| 4 | | Availability | | |  |  | | | | |  | | |  |
| 5 | | Reliability | | |  |  | | | | |  | | |  |
| 6 | | Other | | |  |  | | | | |  | | |  |
| Risk of AlterationStatus | | | | | | | | | | | | | | |
| Risk No. | | Alteration Type | | | Possible (Yes or No) | Risk (High, Medium, or Low) | | | | | Likelihood (High, Medium, Low) | | | Risk Calculation |
| 7 | | Accidental (User) | | |  |  | | | | |  | | |  |
| 8 | | Malicious Compromise | | |  |  | | | | |  | | |  |
| 9 | | Corruption (System) | | |  |  | | | | |  | | |  |
| 10 | | Other | | |  |  | | | | |  | | |  |

**Summary Table**

|  |  |  |  |
| --- | --- | --- | --- |
| Risk No. | Data Type | Evaluation Summary | Risk Handling (Avoid, Minimize, Transfer, Accept) & Description |
| 1 | Critical |  |  |
| 2 | Limited-Access |  |  |
| Risk No. | Denial Type |  |  |
| 3 | Degradation |  |  |
| 4 | Availability |  |  |
| 5 | Reliability |  |  |
| 6 | Other |  |  |
| Risk No. | Alteration Type |  |  |
| 7 | Accidental (User) |  |  |
| 8 | Malicious Compromise |  |  |
| 9 | Corruption (System) |  |  |
| 10 | Other |  |  |

**Risk Calculation**

Each risk factor was calculated by assigning numeric value to each of the three columns, “Possible” (“Present” in the case of data disclosure risks), “Risk”, and “Likelihood”. For “Possible”, the values are 1 for “Yes” and 0 for “No”; for “Risk”, the values are 3 for “High”, 2 for “Medium”, and 1 for “Low”; and for “Likelihood”, the values are 3 for “High”, 2 for “Medium”, and 1 for “Low”. Therefore, a score can range from 0 to 9 for a particular risk factor.

**Overall Rating**

The overall rating is the sum of all calculations for all risk factors. This number can range from 0 to 90. A score of 0 to 29 is considered low impact; a score of 30 to 59 is considered medium impact; and a score of 60 or more is considered high impact.

**Written Report**

Please provide a verbose description of each risk factor summary and risk handling method, if necessary.

**Appendix**

**Table 1. Risk Level Definition**

| **Magnitude of Impact** | **Risk Level Definition** |
| --- | --- |
| **High** | There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. |
| **Moderate** | Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. |
| **Low** | The system’s Authorizing Official must determine whether corrective actions are still required or decide to accept the risk. |

**Table 2. Likelihood Definition**

|  |  |
| --- | --- |
| **Level** | **Likelihood Definition** |
| **High** | The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. |
| **Moderate** | The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. |
| **Low** | The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. |