RISK ASSESSMENT REPORT

ACME *11/2/2022*

**Record of Changes:**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Sections Modified | Description of Changes |
| 1.0 | 11/2/2022 | Initial RAR |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Scope**

The scope of this risk assessment is focused on the system’s use of resources and controls to mitigate vulnerabilities exploitable by threat agents (internal and external) identified during the RMF control selection process, based on the system’s categorization.

This initial assessment will be a Tier 3 or “information system level” risk assessment. While not entirely comprehensive of all threats and vulnerabilities to the Intellectual Properties(IPs), this assessment will include any known risks related to the incomplete or inadequate implementation of the NIST SP 800-53 controls selected for this system. This document will be updated after certification testing to include any vulnerabilities or observations by the independent assessment team. Data collected during this assessment may be used to support higher level risk assessments at the mission/business or organization level.

**Purpose**

*Initial Risk Assessment was requested of the Marvin the Martian SOC by the CISO following a large data breach while the Cyber Stooges SOC was outsourced. Risk assessment seeks to outline and qualify what risks can be observed when judged by the NIST 800-53 guidelines.*

**Risk Assessment Approach**

This initial risk assessment was conducted using the guidelines outlined in the *NIST SP 800-30, Guide for Conducting Risk Assessments*. A qualitative approach will be utilized for this assessment, to bridge the gap between teams and management. Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and consequences/impact to mission.

The following table is provided as a list of sample threat sources. Use this table to determine relevant threats to the system.

**Table 1: Sample Threat Sources (see NIST SP 800-30 for complete list)**

| TYPE OF THREAT SOURCE | DESCRIPTION |
| --- | --- |
| ADVERSARIAL   * Individual (outsider, insider, trusted, privileged) * Group (ad-hoc or established) * Organization (competitor, supplier, partner, customer) * Nation state | Individuals, groups, organizations, or states that seek to exploit the organization’s dependence on cyber resources (e.g., information in electronic form, information and communications, and the communications and information-handling capabilities provided by those technologies. |
| ADVERSARIAL   * Standard user * Privileged user/Administrator | Erroneous actions taken by individuals in the course of executing everyday responsibilities. |
| STRUCTURAL   * IT Equipment (storage, processing, comm., display, sensor, controller) * Environmental conditions * Temperature/humidity controls * Power supply * Software * Operating system * Networking * General-purpose application * Mission-specific application | Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters. |
| ENVIRONMENTAL   * Natural or man-made (fire, flood, earthquake, etc.) * Unusual natural event (e.g., sunspots) * Infrastructure failure/outage (electrical, telecomm) | Natural disasters and failures of critical infrastructures on which the organization depends, but is outside the control of the organization. Can be characterized in terms of severity and duration. |

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

**Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)**

| Qualitative Values | Description |
| --- | --- |
| Very High | Adversary is **almost certain** to initiate the threat event. |
| High | Adversary is **highly likely** to initiate the threat event. |
| Moderate | Adversary is **somewhat likely** to initiate the threat event. |
| Low | Adversary is **unlikely** to initiate the threat event. |
| Very Low | Adversary is **highly unlikely** to initiate the threat event |

**Table 3: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)**

| Qualitative Values | Description |
| --- | --- |
| Very High | Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**. |
| High | Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**. |
| Moderate | Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**. |
| Low | Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**. |
| Very Low | Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**. |

**Table 4: Assessment Scale – Impact of Threat Events**

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. |
| Moderate | The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. |
| Low | The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| Very Low | The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. |

**Table 5: Assessment Scale – Level of Risk**

| Qualitative Values | Description |
| --- | --- |
| Very High | Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Moderate | Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Low | Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Very Low | Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |

**Table 6: Assessment Scale – Level of Risk (Combination of Likelihood and Impact)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood (That Occurrence Results in Adverse Impact)** | **Level of Impact** | | | | |
| Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

Risk Assessment Approach

Determine relevant threats to ACME IPs. List the risks to the IPs in the Risk Assessment Results table below and detail the relevant mitigating factors and controls in three differing cost fashions. Refer to NIST SP 800-30 for further guidance, examples, and suggestions.

**Risk Assessment Results**

| Threat Event | Vulnerabilities / Predisposing Characteristics | Mitigating Factors | Likelihood (Tbl 2 or 3) | Impact (Table 4) | Risk  (Tbls 5 & 6) | Cost |
| --- | --- | --- | --- | --- | --- | --- |
| *Data Exfiltration* | *No PLOP* | *Implement PLOP* | *Very High* | *Very High* | *Very High* | *$* |
| Unauthorized Access | IAM is disorganized | Proper IAM | Very High | Very High | Very High | $$ |
| Service outages | No SCM | Implement SCM | High | High | High | $$$ |
| IP loss | Social Engineering | Technical training | Very High | Very High | Very High | $$$ |
| Corporate espionage | Failure to maintain IPs confidential | DMZ, access control | Very High | Very High | Very High | $$$ |

\* Likelihood / Impact / Risk = Very High, High, Moderate, Low, or Very Low