Facility Security Risk Assessment Guidelines

Assessment Process Overview

The Risk Assessment process includes the following steps:

1. Identify the assets.

2. Determine the critical level of assets.

3. Identify the threats to each critical asset.

4. Identify the existing countermeasures (existing security is existing countermeasures).

5. Determine the vulnerability level of each critical asset.

6. Determine the risk level of each critical asset.

7. Recommend security upgrades to reduce high levels of risk.

8. Perform a cost-benefit analysis in support of upgrade recommendation if possible.

Definitions

*Asset* means a person, place, item, or information associated with the operation or function of the facility or organization. Its value may be quantifiable in terms of dollars. The total cost of damage to or loss of an asset is evaluated in the process. This may include replacement cost, repair cost, and the financial impact (consequence cost) of the loss event.

*Loss event* means physical or financial damage to or destruction of an asset. While human life is priceless, the process requires that each asset be given a value.

*Critical level of an asset* is determined by the impact its damage or loss will have on the continued operation of the business and its facilities and personnel. Criticality values are assigned on a scale of 1 through 4. See Rating the Impact of Loss section below.

*Threat* means any action or event, whether human or natural in origin, that can result in a loss event. Determine the probability of a specific threat successfully causing a loss event, not the probability of the threat occurring. This distinction is important and requires that the threats established be credible and realistic. A credible threat assessment and response should be established and is paramount to a successful security assessment. All possible threats, internal and external, must be carefully considered.

*Countermeasure* means any action or combination of actions involving physical, technical, administrative, procedural, or other measure(s) taken to reduce the severity of an identified risk.

Rating the Impact of Loss

The four levels of critical function(s) of an asset are as follows:

**1—Essential:** Total destruction of (or severe damage to) the asset would cause complete loss of business continuity. This is a catastrophic loss.

**2—Critical:** Total destruction of (or severe damage to) the asset would cause severe impairment of business continuity. This is a serious loss.

**3—Important:** Total destruction of (or severe damage to) the asset would cause noticeable impact on business continuity. This is a moderate loss.

**4—Not important:** Total destruction of (or severe damage to) the asset would cause no noticeable impact on business continuity. This is a minor loss.

Asset Vulnerability Rating

The level of vulnerability of an asset is determined by assessing the threats with the existing countermeasures. If the existing countermeasures are effectively protecting the asset from all threats, vulnerability will be low. If, however, the existing countermeasures are not adequate to prevent or withstand an attack, vulnerability is higher. Vulnerability is measured in terms of the probability of a loss event occurring. Vulnerability values are assigned on a scale of A through D. The levels of vulnerability are provided below.

Interpreting Probability of Loss

**A—Extremely high:** The magnitude of the vulnerability is such that if a threat occurs, there is an extremely high probability that it will be successful in causing a loss event.

**B—High:** The magnitude of the vulnerability is such that if a threat occurs, there is a high probability that it will be successful in causing a loss event.

**C—Medium:** The magnitude of the vulnerability is such that if a threat occurs, there is a medium probability that it will result in a loss event.

**D—Low:** The magnitude of the vulnerability is such that if a threat occurs, there is a low probability that it will result in a loss event.

Combine the criticality and vulnerability data associated with specific assets in such a way as to indicate the combined severity of impact and the probability of a loss event occurring. The criticality and vulnerability ratings assigned to the major assets are entered in a risk category chart to determine the overall risk probability rating as shown below.

**Risk Categories**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** **Vulnerability and Criticality** | **1 Essential** | **2 Critical** | **3 Important** | **4 Not Important** |
| (A) Extremely High  | 1A | 2A  | 3A  | 4A  |
| (B) High  | 1B | 2B  | 3B  | 4B  |
| (C) Medium  | 1C | 2C  | 3C  | 4C  |
| (D) Low  | 1D | 2D  | 3D  | 4D  |

The risk assessment chart allows an employer to identify the most likely security risks with the highest potential severity in order to prioritize resources for security upgrades. This table indicates how the risk categories may be interpreted.

**Risk Matrix Management Guide**

|  |  |
| --- | --- |
| **Asset Risk Category** | **Interpretation** |
| **1A 1B 1C 2A 2B 3A** | **These risks are very high and it is recommended that measures be taken to eliminate them.** |
| 1D 2C 2D 3B 3C | These risks are moderate. Management may determine to address these risks. |
| 3D 4A 4B 4C 4D | These risks are low. |

Security Recommendations

Once the level of risk is determined for each asset, recommendations for security upgrades are made, if warranted. The first goal of the upgrades is to reduce the level of risk to those assets that are in the very high category to the greatest degree practicable.

A secondary goal is to reduce the level of risk to the assets in the moderate category to the greatest degree practicable. If there are constraints that preclude the immediate or near-term reduction of risks, recommendations should include planning and budgeting to accomplish this in the future.

When deciding which recommendations or countermeasures to use, the safety and security stakeholders for the organization need to discuss:

* Their immediate versus long-term needs;
* The feasibility of the addition or installation;
* The budget, including short- and long-term costs of the options; *and*
* How these will fit into the organizational climate and employee culture.

|  |  |
| --- | --- |
| **Risk Category** | **Priority** |
| [Insert text] |  |
|  |  |
|  |  |
|  |  |