**CYB-535 Risk Management Framework Guide**

**Directions:** Selecting a model to use in designing your company's risk management framework may be somewhat intimidating. A recommended approach is to begin by studying the models presented in Topic 4, including NIST, ISO, FAIR, OCTAVE, etc. Then, identify what each offers to the envisioned process. Once you understand what each model offers, you can adopt one or more models to fit your organization's needs. Based upon the selected model(s), address all of the criteria below.

**Part 1: Communities of Interest**

A *community of interest* (COI) is a group of people who operate to address security and privacy needs within the mission of the business or organization. This community can include InfoSec, IT, management, and/or users. Each member is held accountable for managing risks, meaning each member has a strategic role to play that is directly linked to managing risks of information assets.

1. Identify and explain the strategic roles each community of interest must play in managing risks to your company's information assets.

**Table 1. Community of Interest**

|  |  |  |
| --- | --- | --- |
| Name | Role(s) | Responsibilities |
|  |  |  |
|  |  |  |

**Part 2: Risk Management Plan**

**Establish the Context of Risk framework and Risk Process**

Refer to the NIST's "Guide for Applying the Risk Management Framework to Federal Information Systems," or "Guide for conducting Risk Assessment," located in the topic Resources. Then, present/map the steps in which you will:

1. Identify the purpose of the risk assessment.
2. Identify the scope of the risk assessment.
3. Identify the assumptions and constraints associated with the risk assessment.
4. Identify the sources of information to be used as inputs to the risk assessment.

**Risk Identification**

Use Table 2 to perform the following:

1. Identify your company's information assets.
2. Classify and categorize your assets into meaningful groups.
3. Prioritize your assets by overall importance.

**Table 2. Assets Classification**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Information Assets** | **Classification:** Confidential, Private, Public | **Impact on Profitability:** Critical, High, Medium | **Impact on Public Image:** Critical, High, Medium | **Impact on Revenue:** Critical, High, Medium | **Weighted Score / 100** |
| Ex: Web Server # 1 | Public | Critical | High | Critical | 95 |

**Threat Assessment**

Use Table 3 to perform the following:

1. Identify/categorize a minimum of 10 threats and their possible vulnerabilities.
2. Determine which vulnerabilities represent a danger to your organization's assets.
3. Determine which threats are internal and which are external.
4. Determine which threat has the highest probability of success/occurrence.
5. Determine which threat could result in the largest loss if successful.

**Table 3. Threat Vulnerability Assessment**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat** | **Possible Vulnerabilities** | **Internal or External** | **Probability of Occurrence / Success** | **Reputation Loss if Successful** | **Financial Loss if Successful** |
| Ex: Information Extortion |  | Internal | 79% | 56% | 80% |

**Part 3: Risk Analysis**

During this process, assign a risk rating/score to each vulnerability defined in Part 2. Use Table 4 to perform the following:

1. **Asset:** List each vulnerable asset.
2. **Vulnerability:** List each possible vulnerability.
3. **Likelihood:** Indicate the likelihood of the realization of the vulnerability by an attacker (0 to 5).
4. **Impact:** Indicate the impact of this vulnerability on your company (0 to 5).
5. **Risk Rating Factor:** Indicate the result of multiplying asset impact by its likelihood (0 to 25).

**Table 4. Asset Vulnerability Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Vulnerability** | **Likelihood** | **Impact** | **Risk Rating Factor** |
| Ex: Email Server | Email disruption due to software failure | 3 | 3 | 9 |

**Part 4: Risk Evaluation/Report Findings**

Based on the results of the risk analysis and threat assessments:

1. Which risks are acceptable to your company? What can they "live with"?
2. Which risks are unacceptable to your company?