Class Activity: Risk Management, Part 2

## *Objective: Using the company profile provided (see SAM), and your imagination where necessary, complete tasks associated with Risk Management.*

Recall the following figure from pg. 120 in the textbook:

### **Note on Health Laws Security**

Health Acts/Laws, such as HIPAA or Canadian provincial or federal statutes, and related frameworks call for due diligence based on good business practices, for systems handling electronic protected health information (EPHI). Creating an Information Risk Assessment Report satisfies these requirements to analyze risks, formulate appropriate safeguards, and document the risk management decision-making process.

# Part 2: Risk Assessment – Tasks include: Determining Likelihood of Occurance and Determining Risk Level

Table

| **Risk Determination Table** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset/Item No.** | **Threat Name** | **Vulnera-bility Name** | **Risk Descrip-tion** | **Existing Controls** | **Likeli-hood of Occur-rence** | **Impact Severity (a.k.a Asset Impact/Rel-ative Value** | **Risk Level (category OR [Likelihood of Occurrence] X [Asset Impact])** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### Describe Risks

Describe how each vulnerability creates a risk to the system in terms of confidentiality, integrity, availability that may result in a compromise of the system.

Complete the “Risk Description” column in the **Risk Determination Table**.

### Identify Existing Controls

Identify existing controls that reduce the likelihood or probability of a threat exploiting a system vulnerability, and/or reduce the magnitude of impact of the exploited vulnerability on the system. Existing controls may be management, operational or technical controls depending on the threat / vulnerability and the risk to the system.

Complete the “Existing Controls” column in the **Risk Determination Table**.

### Determine Likelihood of Occurrence

Estimate the likelihood that a threat will exploit a vulnerability. Likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access and existing controls; the presence, motivation, tenacity, strength and nature of the threat; the presence of vulnerabilities; and the effectiveness of existing controls.

Refer to this table (or generate your own scale) to use when estimating the likelihood that the threat will be realized and exploit the vulnerability on the system. ***(Note: numbers are used in the book… can use categories or numbers, or both).***

| **Likelihood of Occurrence Levels** | |
| --- | --- |
| **Likelihood** | **Description** |
| Negligible (0.1) | Unlikely ever to occur |
| Very Low (0.3) | Likely to occur two/three times every five years |
| Low (0.4) | Likely to occur once every year or less |
| Medium (0.6) | Likely to occur once every six months or less |
| High (0.8) | Likely to occur once per month or less |
| Very High (0.9) | Likely to occur multiple times per month |
| Extreme (1.0) | Likely to occur multiple times per day |

Categorize threat / vulnerability pairs by likelihood of occurrence, complete the “Likelihood of Occurrence” column in the **Risk Determination Table**.

### Determine Severity of Impact (a.k.a Asset Impact/Relative Value)

Determine the magnitude or severity of impact on the system’s operational capabilities and the information it handles, if the threat is realized and exploits the associated vulnerability. Determine the severity of impact for each threat / vulnerability pair by evaluating the potential loss in each security category (confidentiality, integrity, availability, etc.).

|  |  |
| --- | --- |
| Impact Severity Levels | |
| Insignificant(0.5) | Little or no impact |
| Minor(1) | Minimal effort to repair, restore or reconfigure |
| Significant(1.5) | Small but tangible harm, maybe noticeable by a limited audience, some embarrassment, some effort to repair |
| Damaging (2) | Damage to reputation, loss of confidence, significant effort to repair |
| Serious (2.5) | Considerable system outage, loss of connected customers, business confidence, compromise of large amount information |
| Critical (3) | Extended outage, permanent loss of resource, triggering business continuity procedures, complete compromise of information |

Categorize threat / vulnerability pairs by severity or magnitude of impact, and complete the “Impact Severity” column in the **Risk Determination Table**.

**NOTE: Instead of a category, the textbook uses the weighted-factor asset value for this number.** Therefore, this should not conflict with the Asset valuation done in Part 1… In fact, you could use the Score (Average) from the **Information Asset Valuation and Prioritization** table instead of a category… That’s why I have 1, 2, or 3 by each category.

### Determine Risk Levels

***Risk level is the likelihood of occurrence multiplied by the severity of impact (or value of information asset)***. The final value is subject to the system business and technical owners’ discretion.

**Risk determination**

For each threat / vulnerability pair, assess the following:

* Likelihood of the threat attempting to exercise the vulnerability; DONE
* Magnitude of impact if the threat / vulnerability exploit is successful; DONE
* Adequacy of planned or existing security controls for reducing or eliminating risk;  
  **Note: The project team must decide whether to use only currently implemented controls for this analysis, or to include controls that are budgeted and scheduled for installation, and document that decision in the Report.**
* Resulting risk to the information on the system from the threat and vulnerability.

This table shows the resulting risk level, for each degree of likelihood and each level of severity.

| **Risk Levels** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Likelihood of Occurrence** | **Impact Severity** | | | | | |
| **Insignificant(0.5)** | **Minor(1)** | **Significant (1.5)** | **Damaging(2)** | **Serious(2.5)** | **Critical(3)** |
| **Negligible(0.1)** | Low (0.05) | Low (0.1) | Low (0.15) | Low (0.2) | Low (.25) | Low (0.3) |
| **Very Low (0.3)** | Low (0.15) | Low (0.3) | Low (0.45) | Low (0.6) | Low (0.75} | Moderate (0.9) |
| **Low (0.4)** | Low (0.2) | Low (0.4) | Low (0.6) | Low (0.8) | Moderate (1.0) | Moderate (1.2) |
| **Medium (0.6)** | Low (0.3) | Low (0.6) | Moderate (0.9) | Moderate (1.2) | Moderate (1.5) | High (1.8) |
| **High (0.8)** | Low (0.4) | Low (0.8) | Moderate (1.2) | Moderate (1.6) | High (2) | High (2.4) |
| **Very High (0.9)** | Low (0.45) | Moderate (0.9) | Moderate (1.35) | High (1.8) | High (2.25) | High (2.7) |
| **Extreme (1.0)** | Low (0.5) | Moderate (1.0) | Moderate (1.5) | High (2.0) | High (2.5) | High (3.0) |

Combine the likelihood of occurrence with impact severity to derive the risk level for each threat / vulnerability pair. (RISK = likelihood of occurance X impact (or asset value)). Consider the risks to the information on the system, and complete the “Risk Level” column in the **Risk Determination Table**.

# Part 3: Risk Control – Tasks to be determined (see separate document)

#### Sources:

A Risk Assessment Checklist For Small Business (<http://www.comptia.org/Libraries/ME-Misc/The_Purpose_of_Developing_Security_Checklists.sflb.ashx>)

Information Security Risk Assessment Guidelines (http://www.mass.gov/anf/research-and-tech/cyber-security/security -for-state-employees/risk-assessment/risk-assessment-guideline.html)

Principles of Information Security, 4th Edition textbook

NIST SP800-60\_Vol1-Rev1 (<http://csrc.nist.gov/publications/PubsSPs.html>)