Class Activity: Risk Management, Part 3

## *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 3: Risk Control – Tasks include: Select strategy, Justify controls, Implement & monitor controls (implied)

Table 1

| Safeguard Determination Table |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item No. / Asset-Threat-Vulnerability Name**  **(from Risk Determination Table)** | **Control strategy (Defend, Transfer, Mitigate, Accept, Terminate)** | **Recommended Safeguard Description** | **Residual Likelihood of Occurrence** | **Residual Impact Severity** | **Residual Risk Level** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Recommend Controls and Safeguards

Identify controls and safeguards to reduce the risk presented by each threat / vulnerability pair with a moderate or high risk level as identified in the Risk Determination Phase (Part 2).

There are five (5) basic strategies to control each of the risks that result from these vulnerabilities:

Defend – attempts to prevent exploitation of the vulnerability

Transfer – attempts to shift risk to other assets, processes or organizations; insurance, service contracts, outsourcing.

Mitigate – attempts to reduce the impact caused by the exploitation of vulnerability though planning and preparation; incident response plan (IR Plan), disaster recovery plan (DR Plan), business continuity plan (BC Plan).

Accept – the choice to do nothing to protect a vulnerability and accept the outcome of its exploitation; risk levels of low may be addressed by the Accept strategy.

Terminate – directs the organization to avoid those business activities that introduce uncontrollable risks;

When identifying a control or safeguard, consider:

1. Security area where it belongs, such as management, operational, technical.
2. Method it employs to reduce the opportunity for the threat to exploit the vulnerability. (ie. which of the 5 control strategies).
3. Its effectiveness in mitigating the risk to information.
4. Policy and architectural parameters required for its implementation in the environment.
5. Information security category (confidentiality, integrity, availability, access control, audit, etc.) to which the safeguard applies.
6. Whether the cost of the safeguard is commensurate with its reduction in risk.

If more than one safeguard is identified for the same threat / vulnerability pair, list them in this column in separate rows and continue with the analysis steps. The residual risk level must be evaluated during this phase of the assessment and may be further evaluated in risk management activities outside the scope of this project.

If the recommended safeguard cannot be completely implemented in the environment due to cost, management, operational or technical constraints, document the circumstances and continue with the analysis.

Consider control elements implemented as policies and procedures, training, and improved policy enforcement.

List safeguards and controls, with implementation considerations. Complete the “Recommended Safeguard” column in the **Safeguard Determination Table**.

### Determine Residual Likelihood of Occurrence

Follow the directions in the Risk Determination phase (Part 2), while assuming the selected safeguard has been implemented.

Complete the “Residual Likelihood of Occurrence” column in the **Safeguard Determination Table**.

### Determine Residual Severity of Impact

Follow the directions in the Risk Determination phase (Part 2) while assuming the selected safeguard has been implemented.

Complete the “Residual Impact Severity” column in the **Safeguard Determination Table**.

### Determine Residual Risk Levels

Determine the residual risk level for the threat/vulnerability pair and its associated risk once the recommended safeguard is implemented. The residual risk level is determined by examining the likelihood of occurrence of the threat exploiting the vulnerability and the impact severity factors in categories of Confidentiality, Integrity and Availability.

Follow the directions in the Risk Determination phase (Part 2) to determine the residual risk level once the recommended safeguard is implemented.

Depending on the nature and circumstances of threats and vulnerabilities, a recommended safeguard may reduce the risk level to “Low.” Make a note of the situation with a description below the table, if needed, if such special conditions exist.

For new systems, the next steps would include creating a sensitivity assessment, system security requirements, risk assessment report, and system security plan in the SDLC.

Complete the “Residual Risk Level” column in the **Safeguard Determination Table**.

### Cost-Benefit Analysis (not done in this activity)

Organizations must consider the feasibility of implementing information security controls and safeguards. (see pgs. 152-155 in textbook)

SLE (single-loss expectancy) = asset value \* exposure factor (EF), where EF is the percentage loss that would occur from a given vulnerability being exploited

ARO (annualized rate of occurance) is how often you expect a specific type of attack to occur, in # of times per year.

ALE (annualized loss expectancy) = SLE \* ARO

CBA (cost benefit analysis) = ALE (prior) – ALE (post) – ACS (annualized cost of safeguard)

Example: ALE (prior) = $10,000

ALE (post) = $2,000

ACS = $1,000

Answer: $7,000 => benefit is greater than the cost (positive number), so the cost is worth it!

#### 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>)