Assignment-6

Kartik Velede

8672807

Collaborative Environment Processes 1 – INFO8930

Doug Ferrier

June-29-2020

July-07-2020

**Table of Contents**

[**Document Purpose and Mission 3**](#_Toc45052650)

[**Roles and Responsibilities 3**](#_Toc45052651)

[**Program Scope and Boundaries 5**](#_Toc45052652)

[**Criteria 6**](#_Toc45052653)

[**Steps 6**](#_Toc45052654)

[**1. Setup 6**](#_Toc45052655)

[**2. Data Element Inventory 7**](#_Toc45052656)

[**3. Threat Severity 7**](#_Toc45052657)

[**Frequency & Impact Definitions 7**](#_Toc45052658)

[**Frequency & Impact Weightings 10**](#_Toc45052659)

[**Risk Tolerance Level 11**](#_Toc45052660)

[**Threat Severity Analysis 11**](#_Toc45052661)

[**4. Risk Response 12**](#_Toc45052662)

[**5. Mitigated Control Maturity 12**](#_Toc45052663)

[**6. Results 13**](#_Toc45052664)

[**Revision History 16**](#_Toc45052665)

[**References 16**](#_Toc45052666)

# Document Purpose and Mission

This purpose of this document is to describe the process in which threat and risk assessments (TRAs) for VSN-CS are conducted.

This is meant to be part of the larger risk management program for VSN-CS and will align with the goals and objectives set out in the program.

This document is meant to be used in conjunction with the Threat and Risk Assessment Tool to provide repeatable results.

# Roles and Responsibilities

The following individuals are responsible for conducting threat and risk assessments:

**Project Manager:**

Project managers are the first persons to respond to any kind of risk in the business project. The following are some of the responsibilities.

1. Finding out the risks involved in the project
2. Analyzing those risks
3. Preparing strategies to resolve the risks
4. Implementing project risks reduction practices within in the project
5. Resolving the issues that have occurred.

**Risk Manager:**

The following are the responsibilities of risk manager.

1. Implement the procedure that identifies the financial impact to the company, employees, and the customer.
2. The cost-effective programs need to be analyzed to balance the retention.
3. Prepare the financial budget claim rules to give to all the departments in the organization.
4. Gather the information to analyze the risk exposure.

**Subject Matter Experts(SME’s):**

Implementation of risk management rules is done by SME’s. The following are the responsibilities of SME’s

1. Analyze the risk management document and inform project manage for any changes
2. Participate in the scrum meeting of the project risk assessment
3. Review the risk and recommend any changes to project manager
4. Inform about all the new risk to risk manager

# Program Scope and Boundaries

The scope reflects the areas that the risk management program covers and where a threat and risk assessment can occur.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organization (Business Units/Processes)** | **Physical Location(s)** | **Business Data** | **Technology  (IT Systems)** |
| * Category management * Operations * Accounting * Human resources * IT * Maintenance * Customer Service * Workforce Department | * Head office waterloo * Satellite office   Kitchener   * 500 stores across Canada | * Company Database * Accounting information * Sales data * HR * Financials * SharePoint | Applications   * ERP * Replenishment * Budget planning   Backend   * Exchange * SharePoint * MS Link * FTP   Network   * MPLS (includes DSL) * VPN (direct access) |

# Criteria

A threat and risk assessment will be conducted under the following criteria:

* During the access to company’s confidential information such as personal information etc.
* For any projects that involves compliance issues
* Investments of the company which involves more than $5000
* Any activities that stops the daily tasks of the business.

# Steps

All steps of this project are meant to be completed in the Threat and Risk Assessment Tool, as the project is completed from start to finish.

## Setup

1. VSN’s will classify the data within scope of the risk assessment using the following table, which will also be inputted into the Threat and Risk Assessment Tool. This table will also be used for any future risk assessments as well

**Table N. List of data classification levels**

|  |  |
| --- | --- |
| **Classification Level** | **#** |
| Top Secret | 1 |
| Confidential | 2 |
| Internal | 3 |
| Limited | 4 |
| Personal | 5 |

1. System elements will also be identified and input into the Threat and Risk Assessment Tool.

## Data Element Inventory

1. A tool will consist of all the data types.
2. Classification of data is done based on the data types.
3. Mapping of data is done to the existing element whether data is in rest or transit.

## Threat Severity

Based on the threat severity that involves in the company an analysis will be conducted. VSN has identified impacts that involve in the organization and the overall analysis affect.

### Frequency & Impact Definitions

All the identified threats will be assessed to ensure if there is risk involved in or not. Threats will be evaluated based on the frequency and the impact. Current frequency and the expected threat are evaluated to analysis the frequency. Information and recoverability are used to evaluate the impact. The below are the following definitions.

**Table N. Definitions of current frequency rankings**

|  |  |
| --- | --- |
| **Ranking** | **Definition** |
| Never | N/A |
| Once per year | N/A |
| 1x six months | N/A |
| Once per quarter | N/A |
| Once per month | N/A |
| Once per week | N/A |
| Once per day | N/A |
| Constant | N/A |

**Table N. Definitions of expected trend rankings**

|  |  |
| --- | --- |
| **Ranking** | **Definition** |
| Quickly decreasing | There will 50% decrease in the next year |
| Decreasing | There will be less than 50% decrease in the next year |
| No change | No change |
| Increasing | There will be less than 50% Increase in the next year |
| Quickly increasing | There will be 50% increase in the next year |

**Table N. Definitions of functional impact**

|  |  |
| --- | --- |
| **Ranking** | **Definition** |
| None | All the service is provided to the user by the organization |
| Low | All the critical services are provided to the user by the organization. |
| Medium | Only few users are served with critical service by the organization. |
| High | No services is provided to any users |

**Table N. Definitions of information impact**

|  |  |
| --- | --- |
| **Ranking** | **Definition** |
| None | There is no loss of information. |
| Low | There is loss of limited amount of sensitive information. No actions or penalties is required. |
| Medium | Moderate amount of information is lost. Action need to be taken and penalties are given out. |
| High | There is loss of large amount of information. Severe action needs to be taken and there will financial loss to the company. |

**Table N. Definitions of recoverability impact**

|  |  |
| --- | --- |
| **Ranking** | **Definition** |
| None | No effort is required for recovery |
| Low | Need of raising the help desk ticket |
| Medium | Internal resources can be used for recovering. |
| High | Internal and external resource support is required for recovering.  Not recoverable. |

### Frequency & Impact Weightings

The following table show the impact of the frequency and the impact weightings.

|  |  |
| --- | --- |
| **Frequency/Impact Weightings** | **Percent** |
| Frequency | 50% |
| Impact | 50% |

|  |  |
| --- | --- |
| **Frequency Sub-Weightings** | **Percent** |
| Frequency | 50% |
| Expected Trend | 50% |

|  |  |
| --- | --- |
| **Impact Sub-Weightings** | **Percent** |
| Functional Impact | 33% |
| Information Impact | 33% |
| Recoverability Effort | 33% |

### Risk Tolerance Level

VSN’s risk tolerance level is 15%. This means the risk that can be accepted on a project.

### Threat Severity Analysis

1. The criticality will be identified for each asset.
2. The critically level will be identified as W for each asset.
3. Threat identification used by the VSN company is STRIDE. Microsoft developed STRIDE and stands for
   1. **S**poofing
   2. **T**ampering
   3. **R**epudiation
   4. **I**nformation Disclosure
   5. **D**enial of Service
   6. **E**levation of Privilege
4. Stride will be used to analyze the frequency and the impact of the threat.
5. With each STRIDE threat, the frequency and impact of that threat will be analyzed.

## Risk Response

1. The action taken after risk is defined below for each stride threat and system element.

* No risk exists – When the threat is not accepted.
* Accept the risk – Threat is accepted
* Mitigate the risk -Threat is controlled by the security measures.

1. Counter measures needs to be identified.
2. If “Mitigate the Risk” is chosen, then the corresponding counter measures will be identified as well as their specific maturity.

## Mitigated Control Maturity

1. System elements are mapped with STRIDE threat with controls
2. The frequency and impact changes in the threat are identified by each threat and system element
3. VSN company has tools to identify the severity threats from naked threat severity to the mitigated threat severity.

## Results

The results will be evaluated based on its relation to the risk tolerance level.

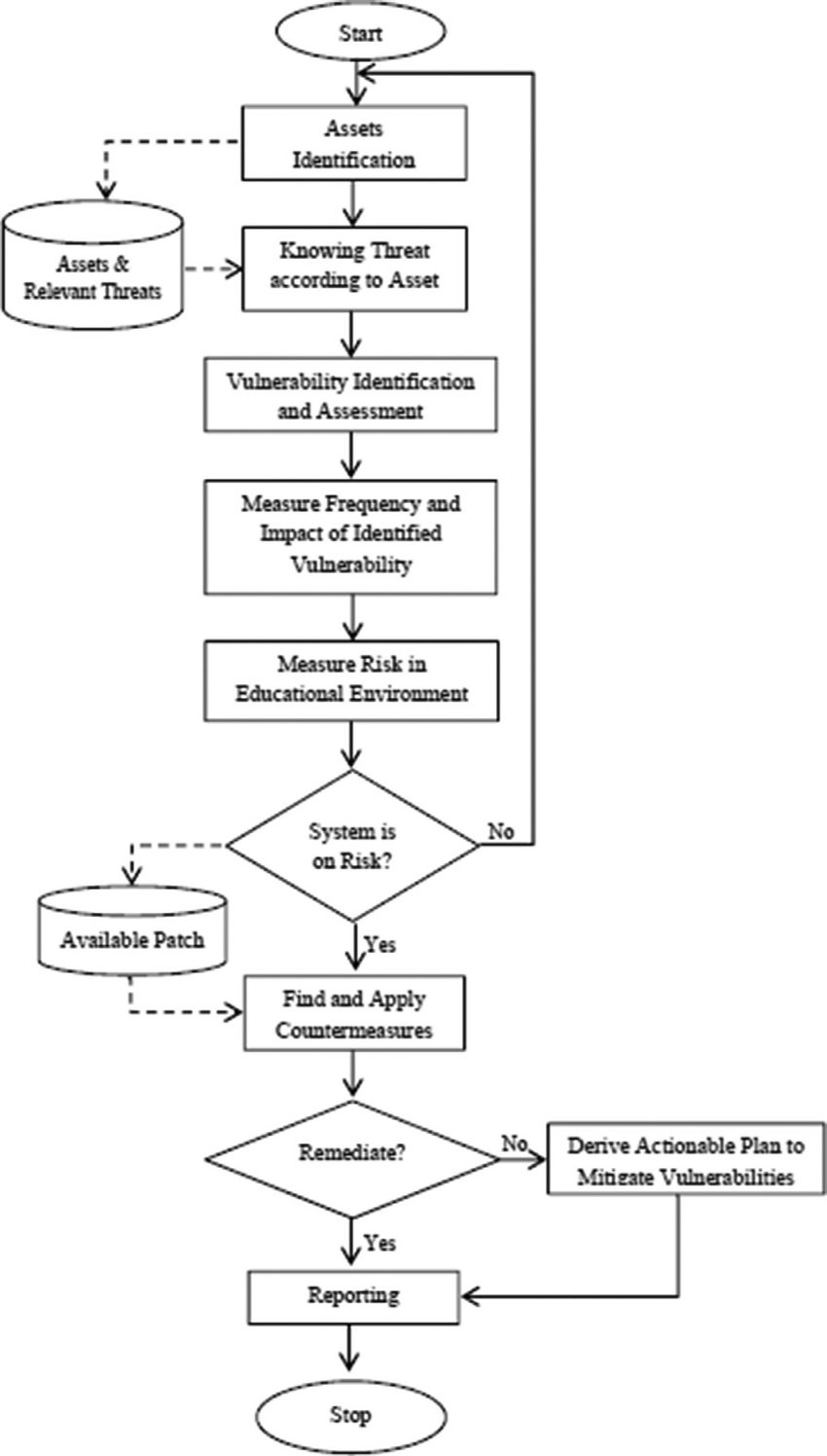
|  |  |  |
| --- | --- | --- |
| Project Risk | Potential Action | Notes |
| Below risk tolerance | Proceed | The project will be executed as per plan |
| Consider the cumulative risk | Reviewing the project plan documentation to find out any risk involved. If risk is identified below some of the actions are taken. |
| Above risk tolerance | Mitigate | To prevent the risk security measures are taken. |
| Transfer | Their will be transfer of risk |
| Terminate | Project execution is stopped |
| Proceed | The execution of project will be continued since the organization has accepted the risk. The execution can be only continued with the approval from all the stakeholder and risk manager |

After action has been decided the result will be presented to the following stakeholders

1. Risk Manager
2. Business Owner
3. Project Manager

After getting the approval from above stakeholders ,now it can be entered into security risk register. The registered document can be found at [www.vsn.com/risk-assessment/security-risk](http://www.vsn.com/risk-assessment/security-risk) .

Below Diagram shows the flowchart for risk assessment process.



# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Authored by** | **Approved by** | **Ver** | **Notes** |
| 7/07/2020 | Division of Information Security | CISO | 1.0 | Initial draft |

# References

Doroka, S. 0. (1997). *Enterprise Project Management Office*. Retrieved from Sample Risk Management Plan: https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-sample.pdf

Marquette. (1999). *Marquette University*. Retrieved from ROLES AND RESPONSIBILITIES IN RISK MANAGEMENT: https://www.marquette.edu/riskunit/riskmanagement/roles.shtml

Six, T. (2000). *Tensix Consulting*. Retrieved from The 3 Must-Have Roles for Risk Management: https://tensix.com/2018/04/the-3-must-have-roles-for-risk-management/