Graduate Program in Information Science and Telecommunications and Networking
School of Computing and Information
University of Pittsburgh

Lab: Risk Management in Healthcare Organizations

Version 1.2, Last Edited 8/9/2018

This lab is to be completed in pairs of two students.

Group Members: ____

____

Date of Experiment: ____

Read the following guidelines before working in the lab

General Guidelines

You will be working on the core bundle of SimpleRisk application which is a free and open source risk management system. It is a web application developed using LAMP (Linux, Apache, MySQL, PHP) stack. An online demo of SimpleRisk[1] is provided which you can try some basic functionalities such as defining new risks and viewing risk reports (Username: user Password: user). However, we will not be using the demo in this lab since it has limited functionality.

A written lab report is required for this assignment. You should turn in a printed copy of the lab report. Space has been provided to answer some of the questions of the exercises in this lab. However, you should attach extra sheets of paper with your answers for some of the questions. Please label your extra sheets with your name and indicate precisely which questions you are answering. Do not forget to give references to the resources to which you consulted while preparing the report. Direct copying is not allowed. You need to rephrase the cited text and express with your own words.

[1] https://demo.simplerisk.com/

Part I: Objective

The objective of the exercises presented here is to familiarize the students with risk assessment in a healthcare organization, in particular one that has adopted a cloud system and with risk management features available in SimpleRisk, which is an open source risk management system.

Part II: Equipment/Software

In this lab, you will learn to use SimpleRisk web application to manage risks in an organization. SimpleRisk is a web application, which is built based on client-server architecture. You will be interacting with the client application to perform the tasks described in the exercises. To do so, you will basically need a web browser and to connect to the server hosting the SimpleRisk. SimpleRisk supports the current versions of major browsers: Chrome, Safari, Firefox, and Internet Explorer[2].

SimpleRisk server application can run on any platform which can run PHP and MySQL. Supported operating systems for the current SimpleRisk version are Windows 8/10/Server 2012, Ubuntu 13.04/14.04, and CENTOS 7. There are two options provided to users for server application: 1) downloading the required files and setting up the application manually, 2) downloading the virtual machine (VM) pre-installed with SimpleRisk application. For this lab, we will be opting in the second option. Hence you will download the provided VM and simply open the SimpleRisk application, which is already setup for you in the VM (guest machine), via a web browser on your host machine[3]. Therefore, you do not need to worry about the OS and other requirements. For being able to run the VM, you will need a hypervisor software[4]. For this lab, you will use either VirtualBox or VMWare.

Additionally, you will need the sample risk assessment spreadsheets, which are guidelines developed for healthcare provider organizations, provided by the Healthcare Information and Management Systems Society (HIMSS)[5].

[2] https://simplerisk.freshdesk.com/support/solutions/articles/6000156747-what-are-the-requirements-for-me-to-run-simplerisk-

[3] For detailed information about virtualization, you can refer to this article: https://en.wikipedia.org/wiki/Virtualization

[4] https://en.wikipedia.org/wiki/Hypervisor

[5] http://www.himss.org/about-himss

Part III: Installation

Please note that if you are using LERSAIS lab computers, you will find the required files to complete the lab in the “risk management.zip” file on your desktop. If you prefer to work on your personal computer, you can download the files you need from the following pages:

- **Hypervisor** (download one of these):
  - VirtualBox (free and open source hypervisor): https://www.virtualbox.org/wiki/Downloads
  - VmWare (free trial versions):
    - VmWare Workstation for Windows and Linux: https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html?ClickID=drwsz0snyozrbcyttms2nrtb0stobomhmybk
    - VmWare Fusion for Mac: https://www.vmware.com/products/fusion/fusion-evaluation.html
- **Latest free version of SimpleRisk:** https://www.simplerisk.com/download (Select “Use a Pre-Installed SimpleRisk Virtual Machine Image” option and download SimpleRisk Virtual Machine Image for the hypervisor you use)
- **Sample risk assessment spreadsheets**:
  - http://www.himss.org/himss-security-risk-assessment-guidedata-collection-matrix
  - http://www.himss.org/library/health-it-privacy-security/sample-cloud-risk-assessment

You can consult to the following page for several purposes like error troubleshooting, resetting admin password, and user guideline: https://simplerisk.freshdesk.com/support/solutions.

After you download the files above, please follow the instructions given here (If you are working in LERSAIS lab, extract the “risk management.zip” file to access the files you need):

1) First, install the VirtualBox or VmWare to your computer following the instructions given on the download links above.

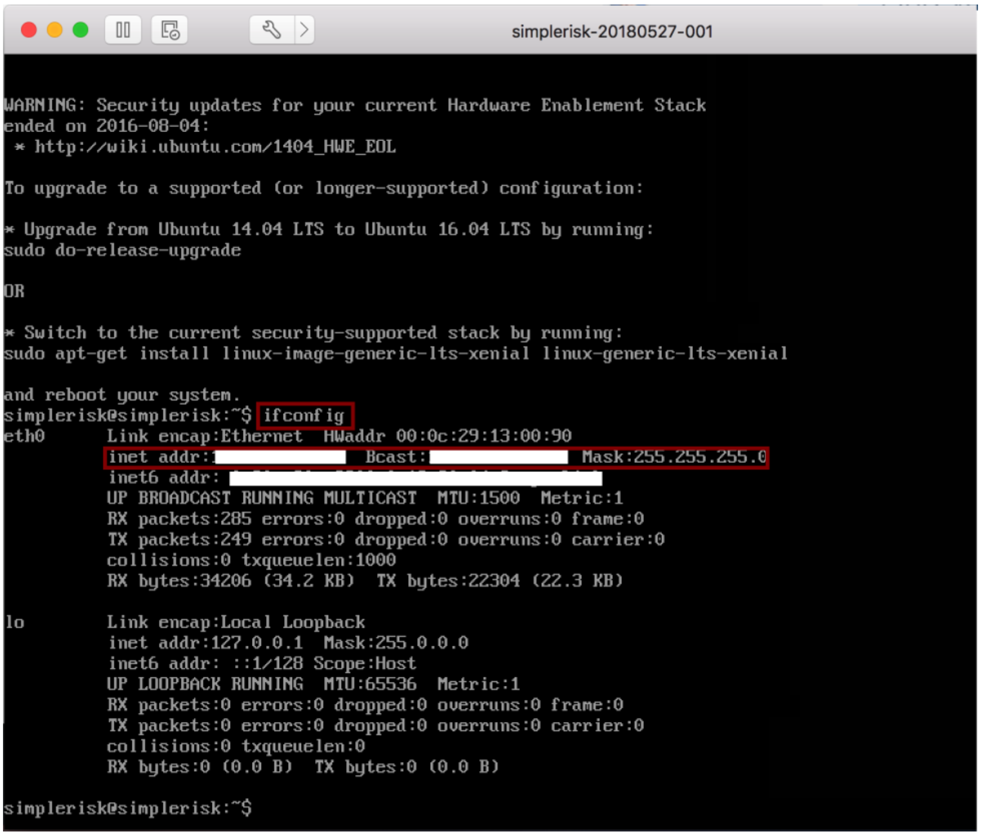
2) Once you install the hypervisor, you need to import the virtual image, which is pre-installed with SimpleRisk application. First, open VMWare or VirtualBox application.
If you work with VirtualBox, you need to select “File -> Import appliance” from the menu at the top and then select the virtual image file (“simplerisk-20180527-001.ova”) from the

directory that the image file is located in. Then you need to click to “Open”, “Continue”, “Import”, and “Agree” in order. After these steps, you will see a window showing the status of import operation. When importing is completed, you can boot the virtual machine by selecting it from the list on the left and selecting “Start” button on the top menu.

In VmWare, process is very similar. You can either select “File -> Import” or “Import an existing virtual machine”. In the dialog box opened, click to “Choose File” button and select the virtual image file. Then proceed until importing is finished. After importing is completed and you click “Finish” button, VM will start booting process.

3) During boot up, you will be asked to enter a passphrase. Enter “simplerisk” as passphrase and hit enter key. Then the VM will complete boot up and ask you a username and password. You need to enter “simplerisk” both as username and password. After login, you will see a warning that says you need to upgrade Ubuntu OS to a higher version or switch to the current secure supported stack (see Figure 1). You will ignore this warning and proceed to the next step.

4) You will start the SimpleRisk server application from the command line of the VM. Type “ifconfig” to find the IP address of the VM. Note the IPv4 address you see on the top part of the list (“eth0” part), as you see in Figure 1. If you are not able to display an IPv4 address after issuing the command, you need to refer to Part VI: Appendix A for troubleshooting.



```
WARNING: Security updates for your current Hardware Enablement Stack
ended on 2016-08-04:
 * http://wiki.ubuntu.com/1404_HWE_EOL

To upgrade to a supported (or longer-supported) configuration:

* Upgrade from Ubuntu 14.04 LTS to Ubuntu 16.04 LTS by running:
sudo do-release-upgrade

OR

* Switch to the current security-supported stack by running:
sudo apt-get install linux-image-generic-lts-xenial linux-generic-lts-xenial

and reboot your system.
simplerisk@simplerisk:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:13:00:90
          inet addr:[redacted]  Bcast:[redacted]  Mask:255.255.255.0
          inet6 addr: [redacted]
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:285 errors:0 dropped:0 overruns:0 frame:0
          TX packets:249 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34206 (34.2 KB)  TX bytes:22304 (22.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

simplerisk@simplerisk:~$
```

Figure 1-Booting the VM and checking its IP address

5) Type the IP address you noted in the previous step, to your web browser in the host machine. Login page of the SimpleRisk application will be displayed. Further steps will be explained in the exercises, as needed.

Part IV: Risk Management in Healthcare Domain

Risk management is a key information security management function for healthcare organizations. There are some regulations/policy frameworks which have been published to protect the security and privacy of healthcare systems and patients and other entities. Those regulations have rules to enforce risk assessment in healthcare organizations.

One of the security frameworks, Health Insurance Portability and Accountability Act of 1996 (HIPAA), was passed as a federal law in the US. It has imposed the responsibility of establishing standards on electronically exchanging health care information to the Department of Health and Human Services (HHS). Since putting health care information online has started to pose risks on privacy of sensitive identifiable information of individuals and security of health care IT systems, HHS has constituted three rules: Security Rule, Privacy Rule, and Breach Notification Rule[6].

[6] https://www.hhs.gov/hipaa/for-professionals/index.html

According to HIPAA Security Rule, healthcare providers need to conduct risk analysis periodically, construct and maintain a risk management plan to secure electronic protected health information (e-PHI)[7]. The period of risk assessment is not defined in the HIPAA Security Rule, but is usually practiced annually [8]. Some of the required steps in risk analysis process per HIPAA Security Rule are: collecting data, identifying vulnerabilities and threats, defining the likelihood and impact of threat occurrence, and periodic reviews[7].

NIST CyberSecurity Framework is another policy framework, which is published by NIST and aimed to guide organizations to manage their security privacy risks, specifically for improving security of the critical infrastructure in the US[9]. There are some security management standards which have rules about risk management like ISO/IEC 27000 family: ISO 27001, ISO 27002. However, these are not aimed for healthcare domain. ISO 80001 is a risk management standard which has been developed specifically for networks of medical devices[8].

Part V: Exercises

Throughout exercises, you will explore risk assessment for a healthcare provider organization specifically the one which has adopted a cloud system. For this purpose, you will consult to risk assessment spreadsheets provided by HIMMS (a general risk assessment guideline for healthcare providers and a cloud specific risk assessment guideline for healthcare providers) and use SimpleRisk risk management system.

Exercise 1: *Managing Users*

In this exercise, you will explore account management in SimpleRisk. You will learn how to use administrator account to add new users to the system, and how to edit and delete user accounts. You will inspect credential and privilege management as well.

Before continuing with exercises in this part, please make sure that you start server application successfully and display Simplerisk on your browser as explained in Part III. Login to admin account with username: “admin” and password: “admin”.

[7] https://www.himss.org/file/1318331

[8] http://www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf

[9] https://www.nist.gov/cybersecurity-framework

Exercise 1.1: Add Users

1. After logging into the system as admin, you will see that the "Configure" tab on top of the screen is selected. On this page, click on "User Management" tab on the left side.
2. When you navigate to user management page, you will see a section: "Add a New User".
3. In this section, fill in the fields as follows:
    a. For "Type" field, leave the default value as "SimpleRisk".
    b. Fill in "Full Name" field with name and surname of group member 1. You do not need to fill in "E-mail Address" field.
    c. Enter "member 1" as value into "Username" field. Fill in password field with "Security2018?". Leave all other fields empty/ unselected and push "Add" button (placed under "Multi-Factor Authentication") to save the new user.
4. If you followed the steps successfully, now you should be seeing the following message "The new user was added successfully."
5. Find the section: "View Details for User" on user management page. Click on the drop-down list labelled as "Details for User". How many users are there in the list, and what are the user names? Show that you added the user by attaching a screen shot to the report.
6. Follow the steps 1 through 3c (including step 3c). This time, enter "test account" into "Full Name" field and "test" into "Username" field.
7. Show that you added the test user by attaching a screen shot as instructed in step 5.

Exercise 1.2: Delete Users

1. Find the section: "Delete an Existing User" on user management page. Click on the drop-down list labelled as "delete current user" and select "test" user. By pressing "Delete" button, delete test user.
2. If you followed the steps successfully, now you should be seeing a message. Show that you deleted the test user by attaching the screen shot of this message.
3. In "View Details for User" section, inspect the user list as described in Exercise 1.1. How many users are there in the list, and what are the user names? Show that you deleted the test user by attaching a screen shot.

Exercise 1.3: Edit User Accounts

1. Go to "View Details for User" part on user management page. Select the user account you defined in Exercise 1.1 for group member 1 and click on "Select" button.
2. On user details page, fill in "E-mail" field and select "English" as the language for this user account. Assign this user to the "Information Security" team from the drop-down list: "Team(s)". Click on "Update" button (placed under "Multi-Factor Authentication") to save the changes.
3. If you followed the steps successfully, now you should be seeing a message. Show that you updated the user details by attaching the screen shot of this message.
4. Go to "View Details for User" part on user management page. Select the user account for group member 1 and click on "Select" button. Show the changes you made by attaching a screen shot.

Exercise 1.4: Credentials

1. Follow the steps 1 through 3b of Exercise 1.1 (including step 3b).
   a. This time, fill in "Full Name" field with the name and surname of group member 2. You should also provide email, language and team information for this user, as you do in Exercise 1.3.
   b. Enter "member 2" as value into "Username" field. Fill in the "Password" and "Repeat Password" fields with the value "password". Leave all other fields empty/ unselected and push "Add" button (placed under "Multi-Factor Authentication") to save the new user.
   c. What message do you get? What should you do to avoid this message?

      ____

      ____

      ____

   d. Define a new password based on the message you get in previous step. You should **only make change** based on the requirement given in the warning message. Then try to add the user again.
   e. What is your new password? ______________________________
   f. What message do you get this time? What should you do to avoid this message?

      ____

      ____

      ____

g. Define a new password based on the message you get in step 3c and 3f. Then try to add the user again.

h. What is your new password? ____

i. What message do you get this time? What should you do to avoid this message?

____

____

____

j. Define a new password based on the message you get in step 3d. Then try to add the user again.

k. What is your new password? ____

2. If you followed the steps successfully, now you should be seeing the following message "The new user was added successfully."
3. Inspect user management page. Which part (bolded heading) do you think that is related to error messages you get steps 1b through 1i?

   ____

   Which of the checkboxes are selected by default?

   ____

   ____

   ____

   Which of them should be checked in order for you not to receive errors with the provided password in step 1b?

   ____

   What are the other features provided for advanced credential management?

   ____

   ____

   ____

4. As instructed in Exercise 1.3, go to user details page for "member 2" and show that you set values for fields required in this exercise by attaching a screen shot.

Exercise 1.5: Privilege Management

You will be configuring user privileges for risk management in this section. Suppose that you are risk management team members. Member 1 has team leader role and member 2 has team member role. Hence, member 1 will have higher level privileges compared to member 2. More precisely, member 1 will have privileges for both risk mitigation and risk assessment whereas member 2 will only have privileges for identifying risks (refer to risk management lifecycle in lecture notes).

1. Inspect user management page. Which part (bolded heading) of the page do you think that is for defining privileges based on risk management team roles?

   ____

2. Go to user details page for "member 1" as instructed in Exercise 1.3. Select the appropriate privileges for this user based on the responsibilities of the user, and attach a screen shot. Do not forget to click on "Update" button to save privilege selections.
   Hint: Groups of privileges map to the tabs user see on top of their home page when they login, like you see for admin account on the top: "Governance, Risk Management, Compliance, Asset Management, Assessments, Reporting, Configure. You should focus on more risk management related privileges. You can login to members' account to make sure that you configure right access privileges.
3. Go to user details page for "member 2" as instructed in Exercise 1.3. Select the appropriate privileges for this user based on the responsibilities of the user, and attach a screen shot. Do not forget to click on "Update" button to save privilege selections.
4. Which group of privileges should not be provided to none of the two members and why? (groups: "Risk Management", "Asset Management", "Assessments", "Configure")

   ____

   ____

   ____

   ____

5. Which group of privileges should be provided to member 1, different than member 2 and why? (Only group/groups, not individual privileges)

   ____

   ____

   ____

Exercise 2: *Asset Management*

Before studying risk management in a healthcare organization using SimpleRisk application, you need to perform asset management. You need to keep track of your assets in order to evaluate impact of vulnerabilities. Those assets can be devices, cloud services, applications, and so on. You should also know which business activities are associated with each asset so that you are able to evaluate the effect of compromise when an incident occurs. In this exercise, you will learn how to define, edit and delete assets in SimpleRisk. You will refer to risk assessment spreadsheets to look up for sample assets in a healthcare organization.

Exercise 2.1: Add Asset

1. Logout from admin account.
2. Which user account do you need to login to do asset management and why?

   ____

   ____
3. Login to the user account that you selected on step 2.
4. Select “Asset Management” tab on the top. Then navigate to “Add & Delete Assets” page by selecting the tab on the left pane.
5. Open “RA03_RA_Guide_Matrix_Final.xlsx” file.
6. Study the Excel file, which is a risk management guideline developed by HIMSS for healthcare organizations.
7. What are the names of two sheets in this file, which include list of sample assets for healthcare organizations?
8. Go back to SimpleRisk and the page where you left in step 4.
   a. In “Add a New Asset” part, enter the name of an asset from the first category of assets you inspected in steps 6 and 7. You can leave “IP Address” field empty.
   b. Assign a range of values to your asset from “Asset Valuation” drop-down list.
   c. Select a team from “Team” drop-down list, which you think is responsible from this asset. Leave all other fields empty/ unselected and push “Add” button.
   d. Follow steps a through c to add another asset from the second category of assets you inspected in steps 6 and 7.
9. Think about two example assets (from both categories you wrote down in step 7) in healthcare organizations which do not reside in the given lists.
   a. Follow steps 8a through 8c to add these two assets.

Exercise 2.2: Edit Asset

1. Go to “Edit Assets” page by selecting “Edit Assets” tab on the left.
2. Attach a screen shot of the list of assets you defined in Exercise 2.1.
3. Fill in “Asset Details” field for each asset and do not forget to press “Update” button to save the changes. You can utilize from spreadsheets to enter details.

4. You can also select a site for the assets. To do this, you need to define site/location other than the default "All Sites".
    a. Logout from the current user account and login to admin account.
    b. Navigate to "Configure" page via related tab at the top and then "Add and Remove Values" page from the tab on the left.
    c. Define at least two sites in "Site/Location" part based on the assets you defined.
    d. Logout from admin account and login to the user account you have been managing assets.
    e. Select "Asset Management" tab on the top. Then go to "Edit Assets" page by selecting "Edit Assets" tab on the left.
    f. For each asset, select the related site/location and press "Update".
    g. Attach a screen shot of the list of the assets.

Exercise 2.3: Delete Asset

1. Navigate to "Add and Delete Assets" page from the left menu. Go to "Delete an Existing Asset" part.
2. Select the assets you defined in Exercise 2.2, which were not originally in the asset list in the guideline file, but you have come up with, and click "Delete" button.
3. Go to "Edit Assets" page by selecting "Edit Assets" tab on the left.
4. Attach a screen shot of the list of the assets.

Exercise 3: *Risk Management in Healthcare Organizations*

In this exercise, you will study risk assessment, specifically risk identification, process in a healthcare organization which has adopted a cloud system. You will explore how to define, edit, and delete risks in SimpleRisk application utilizing sample risk assessment sheets for healthcare organizations.

Exercise 3.1: Understanding Concepts and Policy Conformance

You will explore the two sample risk assessment guidelines in "risk management.zip" file provided by HIMSS. When you extract the zip file, you have the following excel files:

- RA03_RA_Guide_Matrix_Final.xlsx: This is the general risk management guideline for healthcare organizations. It provides template risk assessment matrix, example risks, threats, vulnerabilities, assets and so on, based on some reference documents/standards.

- RA05_RA_Cloud_Computing.xlsx: This is a specific risk management guideline for healthcare organizations which have adopted a cloud system.

1. Open “RA03_RA_Guide_Matrix_Final.xlsx” file.
2. Study the threat sources provided. What are the groups of threat sources presented?
3. Which publication is referred to present this list?
4. Study the two sheets named as “Threat Events (Adversarial)” and “Threat Events (Non-Adversarial)”. What do you think is the difference between threat source and threat events? (Do not copy paste information you found, express in your own words).
5. Study the sheet named as “Vulnerabilities”. What do you think is the relation between vulnerability, threat source, and threat action?
6. Ransomware has become a widely experienced attack to IT systems of healthcare organizations currently[10]. Which of the example vulnerabilities provided do you think might be the most possible cause of a ransomware attack in a healthcare organization?
7. Study the two sheets named as “Score Card Definitions” and “Security Score Card”. What do you think is the use of Security Score Card and its importance for a healthcare organization? (Hint: think about policy conformance)

[10] https://healthitsecurity.com/news/3-tools-to-help-prevent-healthcare-ransomware-attacks

____

____

____

____

8. Study the “Risk Assessment Report” sheet. Pay attention to the columns and recognize the connections of them with your previous investigations. What are the two columns related to your previous investigation?

   ____

9. What are the new fields you recognize in this risk assessment template different than the ones you give as answer in step 8?

   ____

   ____

   ____

   ____

   ____

10. Study the “Likelihood, Impact, Risk” sheet. Which table/information can you utilize to decide the “Impact Severity” for a risk item?

    ____

    ____

11. Based on your investigation in steps 8-10, which additional column could most probably be added into “Risk Assessment Report” sheet and why?

    ____

    ____

    ____

12. Open “RA05_RA_Cloud_Computing.xlsx” file. You will recognize that this file has 3 sheets and two of them has overlapping information with the other risk management guideline file. The sheet “Cloud Computing Risk Assessment” is the sheet specific for cloud technology adoption. Study this sheet, as you will need to refer to it in the sequel.

Exercise 3.2: Defining Risks

1. Login to “member 2” user account.
2. Navigate to “Risk management” page using the tab at the top and then go to “Submit Risk” page clicking the tab on the left.

3. Go to “RA05_RA_Cloud_Computing.xlsx” file and then “Cloud Computing Risk Assessment” sheet. You will be defining the **risk item 1** (row 7) of this sheet in SimpleRisk.
   a. Fill in “Subject” field with “Vulnerability Name”. Use “Risk Description” information to fill in “Additional Notes” area.
   b. Use “Threat Source” information to fill in “Risk Source” area. Please note that you should select the proper source from the drop-down list.
   c. Fill in “Current Likelihood” “Current Impact” areas by considering the mapping of their levels between spreadsheet and SimpleRisk. You will later notice that “Risk Level” is calculated at the background, based on the “Risk Scoring Method”.
   d. Click on “Submit Risk” button to save the risk item. Please note that you will not get a feedback from the application that you successfully added the risk item. Therefore, do not click on “Submit Risk” button multiple times.
   e. Attach a screen shot of the risk details (Please scale it to fit into screen shot, from the start of the details until “Comments” point).
4. Go to “RA03_RA_Guide_Matrix_Final.xlsx” file and then “Risk Assessment Report” sheet. You will be defining the **risk item 2** (row 6) of this sheet in SimpleRisk. Repeat the steps 3a through 3d to define **risk item 2**.

Exercise 3.3: Editing Risks

Exercise 3.3.1 Edit Risk Details

1. Navigate to “Risk management” page using the tab at the top and then go to “Perform Reviews” page clicking the tab on the left.
2. You will see a list of risks which have been defined before. Click the link on the “ID#” column of the **risk item 2** which you have defined in the previous exercise.
   a. The page of the risk item 2 will be displayed. Click on the “Details” tab. Press the “Edit Details” button.
   b. Fill in “Affected Assets” with assets as you think which may be affected from the vulnerability. You can select the assets you defined or type in other assets if the ones you defined are not relevant to this risk item. You can utilize from asset samples in the guideline.
   c. Select “Control Regulation” which is relevant with our use case. Select a “Technology” related to the risk item.

d. Assume that “member 1” is manager of “member 2” and they are both in “Information Security” group. Select “Owner” of the risk as declared in “Organizational Owner” column in the risk management guideline sheet. Select “Owner’s Manager” and “Team”, accordingly.

e. Press “Save Details” button to save the risk item. Attach the screen shot of edited version of the **risk item 2**.

Exercise 3.3.2 Edit Risk Formula

1. Inspect the page of the current risk item (risk item 2). What is the current risk score of it?

   ____

2. Click on “View Risk Scoring Details” link near the risk score. What is the current risk scoring method? What is the formula of it?

   ____

   ____

3. What are the other risk scoring methods provided?

   ____

   ____

4. Logout from the current user account and login to admin account.
5. Select “Configure” tab at the top and “Configure Risk Formula” on the left.
6. Change the definition of classic risk formula from “My Classic Risk Formula is:” drop-down list by selecting the following formula:

   $$Likelihood \times Impact + 2(Impact)$$

   Do not forget to click to “Update” button.
7. Logout from the admin account and login to “member 2” account again. Follow steps 1 through 2a in the previous exercise (Exercise 3.3.1 Edit Risk Details) to display the details of the **risk item 2**. What is the current value of the risk score of the **risk item 2**? Attach a screen shot of the risk detail page.

   ____

Exercise 4: *Risk Mitigation in SimpleRisk*

Once risks are defined, organizations need to make decisions about how to respond to these risks. If a risk is accepted, then it needs to be reviewed and monitored. Otherwise, a risk treatment plan needs to be developed. This process is known as risk mitigation.[11] In this exercise, you will practice risk mitigation process using SimpleRisk.

1. On the "Plan Mitigation" page of the "Risk Management" tab, select the **risk item 2** we have defined in Exercise 3.
2. On the risk details page, go to "Actions" drop-down list and then select "Plan a Mitigation" option.
3. Select a mitigation planning strategy from "Planning Strategy" drop-down list. You can consult to the reference information security guideline document[11] for health care organizations in order to decide the appropriate mitigation planning strategy. (You will find this document among "reference documents" in the risk management.zip folder on your desktop.) Hint: Look to risk treatment strategies in the reference document.
4. Go back to general risk management guideline you have been working through Exercise 3. Inspect the "Existing Controls" and "Recommended Best Practice Control" columns of "Risk Assessment Report" spreadsheet.
    a. Which fields on the risk mitigation page of SimpleRisk should you use to enter the information presented under these two columns?

    ____

    ____

    ____

    b. Fill in these two fields of the risk item 2.
5. Select "Mitigation Effort" and "Mitigation Cost" which you think is appropriate for the risk item 2.
6. Click the button "Save Mitigation".
7. Select "Perform Reviews" tab on the left and take a screenshot of the risk list. Attach this screen shot to show that you planned mitigation successfully.

Exercise 5: Risk Reports in SimpleRisk

In this exercise, you will be exploring some basic reporting functionalities of SimpleRisk. Before starting the exercise, make sure that you have logged into "member 2" user account. Also make sure that you have just 2 risks in the risk list, which you have defined in previous exercises. If you have more risks, please delete them by logging into admin account (Navigate

[11] https://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_Complex.pdf

Configure -> Delete Risks). In the end, you should have risk item 1 without mitigation and risk item 2 with mitigation.

1. Select “Reporting” tab on the top and then “Overview” tab on the left. Which information do the graphs on this page present? Attach a screen shot of the graphs.

   ____

2. Select “Risk Dashboard” tab on the left. Which information do the graphs on this page present? Attach a screen shot of the first six graphs.

   ____

   ____

   ____

   ____

3. Select “Likelihood and Impact” tab on the left. Attach a screen shot of the graph.
4. Select “Risk Advice” tab on the left. Attach a screen shot of the graph.
5. Select “All Open Risks Assigned to Me” tab on the left. Attach a screen shot of the table.
6. Select “Mitigations by Date” tab on the left. Attach a screen shot of the table.
7. Go to “Risk Management” page selecting the tab at the top of the page. Then, navigate to “Perform Reviews” and view the details of **risk item 1** as explained earlier.
   a. On the risk details page, click on “Actions” list and select “Change Status” option.
   b. From “Set Risk Status To” list, select “Closed” option and click on “Update” button.
8. Go back to “Reporting” page. Select “Overview” tab on the left. Inspect the changes on the pie charts after step 7. Attach a screen shot of the graphs.
9. Select “Risk Dashboard” tab on the left. Inspect the changes on the pie charts after step 7. Attach a screen shot of the first six graphs.

Part VI: Appendix A: Instructions for Assigning an IP address to the VM

You have two options to solve the problem of not displaying an IPv4 address after typing “ifconfig” command:

1. You can connect your VM to host-only adapter, instead of using bridged-adapter.
   a. To do so in Mac OSX: https://luppeng.wordpress.com/2017/07/17/enabling-virtualbox-host-only-adapter-on-mac-os-x/
   b. To do so in Microsoft Windows: http://condor.depaul.edu/glancast/443class/docs/vbox_host-only_setup.html
2. You can disable the firewall of the host computer:
   a. For Windows: https://www.lifewire.com/how-to-disable-the-windows-firewall-2624505
   b. For OSX: https://support.apple.com/en-us/HT201642

Warning: Never think of assigning a static IP to your VM manually because you may cause other machines in the network to disconnect and some services to become unavailable. [12]

[12] https://superuser.com/questions/889602/what-happens-if-2-devices-want-the-same-static-ip-address