

Name: Sudipta Halder

Roll: 2021202011

Subject: Information Security Audit and Assurance


Assignment: Self Risk Assessment

Introduction

The intent of this task is to conduct a self-risk evaluation to recognize possible risks and establish risk-management measures. Risk assessment is an important procedure that may assist persons in identifying dangers, evaluating the likelihood and effect of such hazards, and developing methods to limit or eliminate them. We may become more aware of the hazards we face in our everyday lives by doing a self-risk assessment and taking efforts to reduce them. The objective should be to take charge of one's own safety and well-being by undertaking a full risk assessment and adopting appropriate risk management techniques.

Definitions

- **Threat Identification:** Identifying potential threats to humans in a given environment or situation, such as accidents, natural disasters, criminal activities, or terrorism.
 - **Vulnerability Identification:** Identifying vulnerabilities or weaknesses in the human system that could make them more susceptible to harm or danger from identified threats. This could include factors such as age, health status, physical abilities, or environmental factors.
 - **Control Analysis:** Evaluating the effectiveness of existing controls or safeguards in place to mitigate identified threats and vulnerabilities. This could involve assessing emergency response plans, security measures, or safety protocols.
 - **Likelihood Determination:** Assessing the probability of identified threats occurring, based on factors such as historical data, current trends, or expert opinions.
-

- 
- **Impact Analysis:** Evaluating the potential consequences or impact of identified threats on human health, safety, or well-being, as well as potential financial or reputational impacts.
 - **Risk Determination:** Combining the results of the likelihood and impact analyses to determine the overall level of risk posed by identified threats and vulnerabilities.
 - **Control Recommendations:** Providing recommendations for additional controls or measures to mitigate identified risks and improve the overall safety and security of the human system.
 - **Results Documentation:** Documenting the results of the risk assessment, including identified threats and vulnerabilities, control analysis, likelihood and impact determinations, risk levels, and recommended controls, for future reference and ongoing monitoring.

The types of risks that may take place are listed below:

Chronic Illness

1. **Identifying Potential Risks:** Some of the chronic illnesses we can think of are Diabetes, Hypertension (High Blood Pressure), Asthma, Depression and Anxiety Disorders, Cancer.
2. **Likelihood Assessment: Moderate to High.**
Because the above listed health risks are pretty common in nature.
3. **Impact Assessment: Moderate to High.**
Some diseases are very impactful in nature such as Cancer, Diabetes. But rest of the above listed diseases are moderate in nature.
4. **Risk Tolerance determine: Moderate**
 - a. Hypertension is in my family heredity, so there is a moderate chance of getting it.
 - b. Depression and anxiety disorders are less likely to happen since I do socialize whenever it's necessary and take part in outdoor activities.

- c. I don't eat outside generally. But after coming to IIIT-H, mess food has become a part of life. Sometimes mess food is oily and full of masala. And also sometimes they taste very bad. So, we have to order food from outside to fulfill our needs. That can make an adverse impact slowly.

5. Development of Risk Management Strategies:

- a. I generally take part in outdoor activities and exercise regularly.
- b. I try to follow a nutrient rich diet whenever I get the opportunity(generally at home, in IIITH it's pretty difficult to follow a diet. :))
- c. I along with my family members always do regular health checkups so that even if we get any disease, it gets detected at a pretty early stage and we can get medication as soon as possible.
- d. I take all medications exactly as advised by the doctor.
- e. I also perform yoga to control anxiety and depression.

6. Monitor and adjust

- a. I do monitor whether the strategies I'm performing are really working for me.
- b. If the strategies are working i continue them with little enhancement otherwise i change then and take up different strategies.
- c. I also don't overdo anything.
- d. For diet related things, I prefer to follow a diet chart from a dietician and whatever he/she says, I try to follow it.
- e. I also try to leave a relatively simpler and peaceful life to get rid of anxiety.

Professional Risks

1. **Identifying Potential Risks:** Some of the accidents I can think of are Road Financial Risks, Job Security Risks, Liability Risks, Reputation Risks.
2. **Likelihood Assessment: Low to Moderate.**

Due to recession, job security risk is there in the private sector nowadays which may lead to financial risk and reputation risks. So they are all interconnected.

3. **Impact Assessment: Low to Moderate.**

Some accidents are very impactful in nature such as Financial Risks, Job security risks. Rest are all less impactful in nature.

4. **Risk Tolerance determine: Moderate**

- a. I always try to keep myself up to date to avoid Job security risks.
- b. Also, in the near future I have a plan to move to the government sector, so the job security risk is pretty low there.
- c. The chance of reputation risks are very minimal in my case since I'm very honest and ethical in nature.

- d. Also, chances of liability risks are very minimal in my case since I don't fall in the traps of EMI etc.
5. **Development of Risk Management Strategies: Moderate**
- a. I always try to keep myself up to date to avoid Job security risks.
 - b. Also, I keep on changing companies and learn new technologies to avoid job security risks.
 - c. I do my work with utmost seriousness and responsibility so that the chance of liability risk is very minimal in my case.
 - d. I also plan my savings accordingly to avoid financial risks.
 - e. I generally do a good amount of savings for the future to remain tension free and don't indulge in EMI unnecessarily to avoid financial risks.
 - f. Also, I generally buy a thing if I can afford 2X the price of it with my own money.
 - g. I also follow ethics and honesty to avoid reputational risk.
6. **Monitor and adjust**
- a. In case of job loss, try to find a new job as soon as possible.
 - b. Always keep up to date with technologies and business policies to avoid job loss.
 - c. Also, moving to a less stressful sector can be a good option.
 - d. Savings consistently is a way to avoid financial risk.
 - e. We should also invest in shares, SIPs and invest in startups to beat the inflation of our money.
 - f. Also, to avoid reputational risk, we always should follow the path of ethics and honesty.

Accidents

1. **Identifying Potential Risks:** Some of the accidents I can think of are Road Accidents, Slips, trips and falls, burns, sports injuries, workplace accidents.
2. **Likelihood Assessment: Low to Moderate.**
I generally don't go out of home often. So, chances of accidents are rare in my life.
3. **Impact Assessment: Moderate to High.**
Some accidents are very impactful in nature such as Road accidents, Slips, trips and falls. But rest of the above listed diseases are moderate in nature.
4. **Risk Tolerance determine: Moderate**
 - a. I always try to move on the road with utmost care to avoid road accidents.
 - b. Also, I wear helmets and proper safety gears when I'm riding bikes.

- c. I try to be extra careful when seeping through slippery surfaces.
 - d. Also, during sports events I wear proper shoes and sports gears to prevent injuries.
- 5. Development of Risk Management Strategies: Moderate**
- a. I wear helmets and proper safety gears when I'm riding bikes.
 - b. During sports events I wear proper shoes and sports gears to prevent injuries.
 - c. I obey traffic rules with utmost concentration.
 - d. Try to wear good grip shoes/slippers to avoid slip, trips, falls
- 6. Monitor and adjust**
- Examining to find out if the techniques are truly functioning. We may accomplish this by keeping track of the number of accidents that occur after implementing the aforementioned methods and recalling if we were genuinely following the strategies if an accident occurs (which can occur).

CyberSecurity Risks

1. **Identifying Potential Risks:** Some of the cyber-security I can think of are Phishing, Malware, Ransomware, Password Attacks, Social Engineering.
2. **Likelihood Assessment: Moderate.**

These are pretty common nowadays. I've been a victim of a password attack once on instagram. Also, my PC was once attacked by malware when trying to install a cracked game in windows.
3. **Impact Assessment: Moderate to High.**

Some accidents are very impactful in nature such as Ransomware because it would lead to monetary loss. But rest of the above listed diseases are moderate in nature even though they can have serious impacts such as identity theft, monetary loss etc.
4. **Risk Tolerance determine: Moderate**
 - a. I generally follow a strong password scheme.
 - b. Hence, password attacks are rare in my case.
 - c. Ransomware attack possibility is rare since I use Ubuntu as my primary OS.
 - d. Malware attack also is very rare in my case since
5. **Development of Risk Management Strategies: Moderate**
 - a. I generally follow a strong password scheme.
 - b. Ransomware attack possibility is rare since I use Ubuntu as my primary OS.
 - c. I generally keep my OS up to date due to which chance of different phishing and malware attacks are very minimal in possibility.



- d. Also, I don't use public wifi without a VPN. So, stealing of information through the network is also rare in my case.
- e. Also, I run a script which blocks all suspicious websites, porn websites, advertisements etc. So, chances of these kinds of attacks are very rare.
- f. Also, I block third party cookies to minimize the number of advertisements on websites.

6. Monitor and adjust

- a. I keep my OS up to date so that it can install security patches regularly to keep my system free from malware.
- b. I also keep my script up to date which blocks suspicious websites, advertisements etc.
- c. Also, I generally use VPN when I'm connecting to a public wifi to minimize the chance of information stealing.
- d. Also, I generally try to follow a strong password scheme so that it can't be cracked easily.
- e. I also change the passwords in a regular interval so that it can't be cracked easily.
- f. Also, I don't note down the passwords physically.
- g. Also, I don't save my passwords in any app since we can never trust them. I keep them to myself only.
- h. It is not advisable to access any suspicious website, even if it comes from a reliable source, especially if you are not protected against them.
- i. We should take a backup of our personal data so that in case of ransomware attack, we can be sure that a copy of our data is with us every time.

Conclusion

So, performing a self-risk assessment is a liberating approach to take charge of our health and safety, and it would definitely help us to lead a better life all together.