**Report on Personal Risk Assessment Assignment**

*By*

**Mehnaz Afrose**

**Introduction**

I’m Mehnaz Afrose, MS student of this department. I’m married and have a wonderful son, who is two years and seven months old. My home country is Bangladesh. My parents and other family members are there. Here in the USA, I live with my son and husband. I was not adept in multi-tasking. I was a slow worker and perfectionist, who worked slowly but in a very accurate manner. From this nature I had to change my way of everything in total opposite direction since my son was born. I’m raising my kid all alone and all by myself. I tried to give him in daycare when I got admission here in MS program and started working as a research assistant. It was a massive workload. But daycare didn’t work for him for some reasons. From then, I changed myself to become rabbit from tortoise. I have been managing everything with a single hand, raising a kid, doing chores, studying, research work, and so on. Even right now, I am typing this assignment by keeping my son beside me. Sometimes I can’t manage time to do the submissions on time. But I am very grateful that my professor is very considerate. But some recklessness has added to my calm nature. I must rush through everything to manage this huge load of duties. Even in driving, I wanted to make everything perfect and everything on time. One day I was rushing to a meeting with my supervisor. I was driving almost 90miles/hour. Consequently, I had an accident while taking the exit, I couldn’t control the speed enough for that exit. I was very fortunate that nothing major harm happened to me, but that accident did cost me huge. I had to manage money to fix the car, as my car insurance was not for full coverage because of the financial condition, but later it did cost me more. My studies and at the same time my work were almost over and my whole future was stopped because of one careless impulse of my mind. It was quite a life lesson of being impulsive. I learned nothing is more important than being alive.

When I came here to the USA, I couldn’t bring my laptop with me. So, I brought an external hard disk carrying all my documents, wedding pictures and videos, childhood pictures, and other files. After coming here, I thought this is a safe country, nothing bad will happen if I lost my drive. Instead, I had to keep this hard disk in a safe place and back up all the data in another safe place. Also, I started to use this disk as a pen drive carrying everywhere with me because I couldn’t manage enough time to buy a pen drive. One day it got lost. I was freaked out and started realizing how naïve and unwise I was. Thankfully I was able to find it after a while. I didn’t waste more time and backed up all my data in my google drive.

Everyday I walk home from the library. It is one of my basic health routines. As I am diabetic, I ensure walking at least thirty minutes a day. While I walk, I carry my laptop with me in the backpack hanging from my shoulder. One day I was walking down the street, listening to a horror story with my earbud stuffed into my earhole. I didn’t realize some passerby was following me riding his bicycle. Suddenly he snatched my backpack and eloped from eyesight within a blink of an eye. I lost my laptop and other valuable belongings that day. I realized; I shouldn’t carry valuables while walking down the street. If I need to carry something important, I should have taken a safe ride. In the google drive I had a back up everything, so most of the data was restored. But losing a laptop cost me money. Very recently I learned about ‘prey’, a tracking software, by which I can recover my lost devices. I wish I had known earlier.

I am prone to phishing attacks. Also, I can’t differentiate between the actual email or links and the phishing emails or links. This is testified from the exercise “Have I been Pwned and Phishing attack”. By doing this assignment I took part in two phishing quizzes where I had to identify which emails are real and which are phishing. My score was not satisfactory. Apart from that I was a victim of phishing attack also. A couple of months ago I received a text message from one of my Facebook friends via messenger. The text message contained a link claiming that a famous apparel brand is giving a huge discount. Unfortunately, that brand was my favorite one, and I was a regular customer of theirs. It was hard to ignore the temptation at first. I just wanted to check whether it is real. I clicked the link, and there were consequences.

All these experiences suggest a lower risk tolerance, given the real-life situations I have faced and their impact. Instances like the car accident, the loss of the external hard disk and laptop, and falling victim to phishing attacks have significantly affected my daily life, both emotionally and financially. These events seem to have instilled a greater sense of caution and an awareness of the consequences of taking risks. Thus, my tolerance for risky situations appears to be lower, prompting a more careful and considered approach to daily activities and decisions.

The subject of the inventory and risk assessment focused on evaluating my personal assets and the risks they carried. It was a thorough examination that was categorized within six categories: people, data, hardware, software, routines, and networking tools. Each item was scrutinized to uncover weaknesses and potential threats, following the NIST Risk Management Framework and the CIA (Confidentiality, Integrity, Availability) triad principles. The goal is to grasp how vulnerable these assets are to breaches, unauthorized access, or disruptions, gauging the possible impact on their secrecy, reliability, and accessibility. Ultimately, this assessment aimed to build a solid defense system, mitigating risks, and ensuring the overall security of my inventory.

**Question 1: what did I do?**

**How the inventory was conducted**

Before doing risk assessment, I created an inventory for almost all my information assets and identified threats. The assets were categorized into six categories: people, procedure(routine), hardware, software, data, and network.

Crafting my personal asset inventory became a dedicated endeavor that demanded substantial time and attention. For almost a week, I meticulously combed through every facet of my life, methodically documenting each asset I possess, from the devices I use daily to the routines ingrained in my lifestyle.

My strategy involved keeping an ongoing list readily accessible on my computer. Throughout my daily activities, if something struck me as an asset, I swiftly added it to this evolving inventory. For instance, while engrossed in crafting a training module on Canvas.com, an online platform for educational modules, I realized the wealth of student data and course materials it harbored, qualifying it as both a software and data asset.

Similarly, the beckoning notifications from Train Traq led me to identify this online training portal as another software asset, housing its own trove of valuable data. Yet, the most comprehensive source proved to be my cellphone, housing a staggering 48 software assets and an array of data categories.

My television, serving not just for entertainment but as an information repository, emerged as a hardware asset. It stored personal data from various streaming services. Even household appliances like smart sensors, security cameras, and the Nest Hello doorbell found their place in my inventory as hardware and networking assets.

For listing people assets, I looked down my family tree, photo albums, Facebook friend list, and my contact information. For identifying routine procedure, I opened my daily activities which I keep recorded in google calendar. Thai is how I identified people, system/procedure assets into my inventory.

Some assets are grouped based on their functionality. For example, memory card, external hard disk, floppy disks all of them I use for keeping the backup of my files and other documents. So, I listed them in a one single entity.

For the routine activities, each routine activity is a combination of multiple activities. So, I picked the common name as a set of all the activities listed in it and added this single activity as a procedure asset. For example, I put an entity naming it self-care. Within this I have a set of activities, such as skin care, hair treatment, manicure, pedicure, doing my nails, etc. Self-care represents all the activities I just mentioned.

When I have something that fits into different groups, I take a good look at what it does best or where it's most important. For example, if it's a tool that helps both with work and with personal stuff, I figure out which role it plays more often or where it's more crucial.

I have an asset named "Sarwar Millat" listed under the "People Category Asset." Now, Sarwar is not only a friend but also someone I collaborate with on certain work-related projects occasionally. In this case, Sarwar falls into both the "Friends" subgroup and the "Colleagues" subgroup within the "People Category Asset." But he is more significant as my best friend than my colleague. So, I put him as my best friend.

That is how the inventory was conducted.

**How assets were categorized**

The categorization of assets involved systematically grouping them into different categories based on their characteristics and functionalities. For instance, assets like my driving license and social media applications were classified under data and software categories, respectively. Meanwhile, routine activities, such as my evening walk routine or regular video calls with family, fell into the routine procedures category.

Arranging assets in this structured manner allowed me to categorize them according to their nature and purpose.

**How threats/vulnerabilities were identified**

In identifying threats and vulnerabilities, I leaned on the NIST Risk Management Framework, with a particular focus on the CIA (Confidentiality, Integrity, Availability) triad. This involved diving deep into different asset categories, carefully weighing potential risks associated with unauthorized access, data manipulation, service disruptions, or breaches. For instance, when I used this framework to assess my driving license, which falls under the Data category, it revealed risks concerning its confidentiality, integrity, and availability. For instance, there's a risk of Identity Theft (confidentiality) if the license isn't kept secure. Tampering with the license information (integrity) could be another issue. Also, the inconvenience caused by losing the physical copy (availability) might lead to additional time and resource expenses for a replacement.

**How assets were prioritized and valued**

The way I assessed and prioritized assets depended on how important they were in my daily life and the potential fallout if they were at risk. I analyzed the role, significance, and the possible risks of each asset. Take, for example, the communication apps I use: WhatsApp, Telegram, Gmail, Outlook, Facebook Messenger, and Text Now. These applications are part of the system because they are inevitable for day-to-day communication and storing important data. The impact of these applications on my routines and data management made them stand out as significant assets in need of protection.

**How systems were determined**

Determining systems within the inventory involved evaluating the collective impact and interconnectedness of assets on my daily activities. When I was determining what constituted systems in the inventory, I looked closely at hardware devices like memory cards, external hard disks, and floppy disks. These devices were grouped together as a system because they played a connected role in storing and safeguarding data. Their collective function was vital in managing and securing information within the inventory, which is why they were categorized together. Same as for communication applications like WhatsApp, Telegram, Gmail, Outlook, Facebook Messenger, and Text Now were identified as systems due to their collaborative function in enabling communication and storing important data, and same as for other categorized assets.

**Question 2: What were the results?**

**Risk assessment of an asset from the People category:**

For the risk assessment, I did the assessment for myself first. I considered my monetary value 1000. This number is a metaphoric number to present myself withing the maximum limit of one thousand. The ID number of this asset is 201 and the system ID is p39. Under the threat/risk category ‘Availability’, my risk value is 30, when it comes to the vulnerability for phishing attack. It is a vital priority. In this case my ARO, .1. That means the probability of occurring of this incident is medium. My tendency to response in any kind of phishing approach is fifty percent. I cannot guarantee that I will not respond to such an attack, or I will be successful in identifying them. That is why I put uncertainty 0.5. I feel l need more rigorous cybersecurity training to increase my awareness and knowledge about phishing attacks. If I apply this plan, I can control the effectiveness up to 80%.

In the integrity category, I added two types of vulnerabilities. One is reckless driving, and another is alcohol and drugs. For reckless driving the priority is vital, ARO is high (.15). That means I am prone to reckless driving. I need to control this urge when I am in some kind of rush for any meeting or any appointment. After my previous car accident, I believe my tendency to drive carelessly has reduced up to 60%. That is why I put the value 0.4 for uncertainty. My calculated risk value is 42, which I don’t want to risk paying. So, I added the action plan AP2, which describes this, I need to be careful, keep calm and quiet while driving. Most importantly I need to keep in mind that nothing is more important than being alive. I also should get full insurance coverage for my car to avoid more monetary loss.

Another integrity category is alcohol and drugs. Very recently I was a breast-feeding mother. That is why I don’t do any kind of drug or alcohol. That is why my risk factors are low in this category. But in the future, I might have some drinks, maybe with some friends, as the breast-feeding period is over now. So, I put my uncertainty very low (0.1).

In the confidential category, my vulnerability is most of my Facebook posts are public. Since nothing serious happened for my public posts, I added the priority as low. With the same reason my uncertainty for publishing posts publicly is .8. I also consider that there can be some unwanted consequences if someone misuses my posts or pictures. So, I added an action plan AP4.

**Risk assessment of an asset from the Process/Routine category:**

To do the risk assessment for a routine asset, I decided to do this for the Evening walk routine, ID 161, system ID Pr8. This is the routine of my daily walk home from the library. The risk priority in available category is vital because in this routine I always carry my laptop in my backpack, and it could be snatched by some attacker. I set the asset value at 50 assuming the price of the laptop. As I am still doing this, in that case the uncertainty is .5, and ARO I set .5. That indicates that the chance of occurrence, in my belief, is medium. My risk value in this case is 5.625 and I am not willing to take that risk of spending this amount of money if I lose my laptop. So, I accepted the action plan AP5, which is: Should use safe ride when carrying valuables, like laptop. Otherwise, don't carry it while walking, and have insurance coverage.

If my laptop/any other valuables are lost by doing this routine work, in that case confidentiality category would be compromised, whose risk priority is medium. Because my laptop is password protected. In that case the ARO of the risk of security password can be cracked, and all the files can be exposed is medium (0.1). As sometimes I carry my laptop in this manner, the uncertainty is 0.65. The risk value of this security compromise is 2.97. So, to avoid this I created the action plan AP6 which always uses strong passwords to protect those devices that I carry with me.

Same as for integrity category compromise risk. To protect the important documents which are stored in some kind of devices which I must carry with me, should encrypt, so that if any document is misplaced and be in the hand of some unauthorized parson, he or she can not abuse those.

**Risk assessment of an asset from the Data category:**

For this part I analyzed the risk value of my driver’s license, one of my the most vital data, ID no. 91, system ID no. D33. This is an asset which represents my identity. That is why I put the asset value 40. In case of confidentiality compromise, it can happen by identity theft, someone could steal my license and use it as her own. I considered this risk might happen very rarely. So, the IRO is .05. If I keep it safe and have duplicate copy of my information (picture of it, or photocopy), controls effectiveness can be 0.8 and uncertainty is .025, which is very low. If I don’t want to take the risk to lose it, I took the action plan AP8, which is improved storage with added security layers to safeguard personal identity information against theft.

In the case of data alteration, which is integrity compromise, this event is also rare. So, the ARO is very low, controls in effect are high, and uncertainty is .04. I added the action plan AP9, which is same as AP8.

In availability compromise, I could lose the physical copy of my driver’s license, or it could be destroyed somehow. I set this risk priority is medium. ARO is also medium, uncertainty is .1.

Either someone stole my driver’s license, I can call 911 and provide my license number to clock it, before the thief could use it. Also, for any physical damage of it, I can issue another copy of it from DMV office. But this would cost me time, gas, and extra money. So, I must be careful always handling it, which is action plan AP10.

**Risk assessment of an asset from the Software category:**

I did the risk assessment for software WhatsApp, Telegram, Gmail, outlook, Facebook messenger, Text now, which are the communication application, asset ID 136, system ID S44. I set the asset value 75, because these applications I use for day-today communication with my people asset domain and for my social media activities. The priority vital because if there is Weak passwords, phishing attacks, social engineering attacks, then it would compromise confidentiality and the consequences would be deteriorating. For this ARO is .2, which is very high. Controls in place should be using strong password requirements, multi-factor authentication (MFA), user education. If these measures are taken, then the controls effectiveness can be .7. For me the uncertainty is 0.5. There is a 50% chance that this occurrence can happen for me. To avoid the risk value 6.75, I should consider the action plan AP11, which is to implement additional access controls and data encryption measures, avoid temptation from phishing links.

The risk priority for integrity compromise is medium and the vulnerability can be unauthorized modification or destruction of personal information. ARO is .1, which is medium. Control effectiveness is 0.7, and uncertainty is 0.3. To avoid the risk value 2.925, I must consider the action plan AP12, which is having regular cybersecurity knowledge, educations, and try best practices.

The risk priority of compromising availability of service because of hacking, or other disruptions can cause temporary or permanent block of the account is low. The reason behind it is I have never faced such incidents. So, the ARO is .05, which is low. Controls in effect can be 065, my uncertainty can be 0.01. Although this is a low priority, I set an action plan AP 13 if any day this might happen. The controls needed are to implement additional redundancy and load balancing measures.

**Risk assessment of an asset from the Hardware category:**

In this section I did the risk assessment for Memory card, external hard disk, floppy disk, these all are from hardware asset category. Asset ID 55, system ID H17. The asset value is 25. Confidentiality compromise is medium. These devices contain sensitive personal information. Any unauthorized access can cause severe damage by exposing sensitive personal information along with other misuse. For me the priority can be medium because I keep these in safe place, and for the vital the documents, I use encryption. For the same reason the ARO is medium (0.1), controls effectiveness is 0.85. There is a risk factor 0.45, and to avoid this I set an action plan AP14: Implement security measures, such as keeping these devices hidden in safe places, use strong password protection.

For the compromise of availability, I set the priority is vital. These hardwires could be lost, or theft. There is always a chance for this if fifty percent. So, the ARO is .5, controls effectiveness is 0.65, and for me the uncertainty is 0.5. To avoid the risk factor, which might cost 6.56, I need the action plan AO15: Should stop carrying with me, keeping backup of the data.

For the case of integrity compromise, while any document stored in these devices could be lost or tempered for carelessness, or unauthorized access. The priority for this is very low for me because I always try to be careful when use to save, edit, or delete data and keep these safe. That is why ARO is low (0.05), controls effectiveness is 0.8, uncertainty is 0.01. There is also an action plan AP16: Being careful when saving other data, check the data is any kind of virus or not. By which the risk value 0.2525 can be reduced.

**Risk assessment of an asset from the Network category:**

For the las section of assessment, I did it for my Alexa home device. This is a smart home assistant. This is a network asset. Asset ID 147, system ID N3. The asset value is 25. For the confidentiality compromise, which can occur by unauthorized access and information leakage, is low. Because this never happened to me, there might be a possibility. So, the ARO is very low (0.001). As there might be a possibility for this vulnerability, I set the numbers for both controls effectiveness and uncertainty 0.5. To avoid this possibility of vulnerability there is an action plan AP17: Update default settings, Continuous monitoring.

Likewise, confidentiality compromise, integrity compromise for this device is also low in case of vulnerability weaknesses in software could allow tampering or compromise. Controls in place can be Keep update the software system. All other numbers are the same as the previous category for the same reason. To avoid this possibility of vulnerability there is an action plan AP18: Update device's software system.

For the availability compromise can be happen for the physical damage and lost. The priority is low. Because I have a toddler who loves to throw things everywhere, and when Alexa responses it attacks his attention. But the priority is low because I always keep this device out of my kid’s reach. So, the ARO is 0.1 (medium). Controls effectiveness is 0.5 and uncertainty is 0.6, as sometimes my kid grabs it somehow. The risk value is 2, which can be avoided by implementing the action plan AP19.

**How I categorized and analyzed one system**

When I sorted through my inventory, I paid close attention to how certain assets connected and influenced my daily routines. Take, for example, the cluster of communication apps I use regularly - WhatsApp, Telegram, Gmail, Outlook, Facebook Messenger, and Text Now. These apps aren't just standalone tools; they're interconnected and vital for my everyday interactions. They're the go-to platforms for communication, storing crucial information, and managing my social connections. That's why I treated them as a unified system within my Software category (Asset ID 136, System ID S44), recognizing their collective impact on various aspects of my life.

**Question 3: What did I learn?**

My overall risk posture, assessed through meticulous categorization and analysis of my assets, reflects a conscious awareness of vulnerabilities and potential threats across various facets of my life. By scrutinizing people, routines, data, hardware, software, and networking tools, I gained insights into the interconnectedness of these assets and their collective impact on my daily activities. This comprehensive assessment enabled the identification of vulnerabilities such as phishing susceptibility, potential data breaches, and compromises in asset availability. Implementing strategic action plans became crucial in mitigating these risks effectively, emphasizing a proactive approach to bolster security measures and minimize potential vulnerabilities in my personal and professional life.

I seem to have a low appetite for risk, considering my experiences and reactions to various incidents outlined in my risk assessment. Impactful events like the car accident, the loss of valuable belongings, and falling victim to phishing attacks have significantly influenced my risk tolerance. These incidents have heightened my awareness of the potential consequences of risky behavior.

My willingness to accept risk appears quite low due to the profound effects these events had on me. Instances like the accident while rushing to a meeting and the loss of my laptop and external hard disk have made me more cautious. I've taken steps to mitigate future risks, such as implementing tracking software, backing up data on cloud storage, and considering cybersecurity training to enhance my awareness of phishing attacks.

There was a proactive attitude of mine of seeking ways to mitigate future risks, such as implementing tracking software, backing up data on cloud storage, and considering cybersecurity training to enhance your awareness of phishing attacks. These actions emphasize my inclination to avoid future risks by improving my preparedness and security measures.

My approach reflects a desire to prioritize safety and stability over taking risks that could lead to potential harm or loss. Overall, my past experiences have shaped a risk-averse stance, leading me to actively seek measures that reduce exposure to similar risks in the future.