1. I was conducting an inventory and risk assessment of various assets. The first asset I assessed was my father, who is a close family member and deemed vital to my personal and emotional well-being. To conduct the assessment, I first conducted an inventory of all the personal information related to my father, including his full name, date of birth, social security number, and medical records. I then categorized the asset as "Person or my close family member" and assigned a CIA asset value of $2 million due to the high value placed on his confidentiality. Next, I identified the threats and vulnerabilities associated with this asset. The main threats were modifications to his personal information, such as identity theft, being drunk and sharing sensitive information, and memory loss leading to accidental disclosure. The vulnerability was identified as being low due to the low probability of these events occurring. To mitigate these risks, controls were put in place, such as having conversations with him to ensure he understands the importance of keeping his personal information secure and controlling his alcohol consumption to avoid unintentional disclosure. The ARO for these threats was determined to be low at 0.05. Considering the controls in place and the uncertainty of the threats occurring, the overall risk value was calculated to be $22,000. This value indicates that while the risks are low, they still require attention and mitigation. To further mitigate the risks, the action plan ID involves having conversations with my father and working on his emotional wellbeing to avoid memory loss and accidental disclosure. Overall, our risk posture is relatively low, but the asset still requires ongoing monitoring and mitigation to maintain its confidentiality and security.
2. As part of our company's (Wells Fargo N.A.) risk management process, we conducted an inventory and risk assessment of our assets. We identified all assets, including procedures and processes, and categorized them based on their value and priority. We also identified potential threats and vulnerabilities that could impact their confidentiality, integrity, and availability. One of the critical assets we assessed was our backup and recovery procedure, with a system ID of 2 and a CIA asset value of $1 million. The priority of this asset was deemed vital, as any failure or inadequacy in backup and recovery procedures could result in data loss, extended system downtime, and inability to resume normal operations. We assessed the potential threats and vulnerabilities that could impact this asset and found that inadequate backup and recovery procedures or failure to test them regularly could result in significant risks to the company's operations. We determined that the likelihood of such an event occurring was low, with an ARO of 0.05. Currently, we have controls in place, including regular performance and testing of backup and recovery procedures and secure storage of backup data. However, there is still some uncertainty regarding the efficacy of our controls, with an uncertainty rating of 0.5. Based on these factors, we calculated the risk value of this asset to be $22,500. To reduce this risk, we plan to implement additional testing and verification of backup and recovery procedures, periodic review and updating of procedures to ensure they align with current system configurations and data volumes. Overall, our risk posture is moderate, with several assets identified as high-priority and in need of further assessment and risk reduction measures.
3. As part of our organization's risk assessment process, we conducted an inventory of our assets and evaluated the potential risks associated with each. We categorized our assets based on their type, value, and importance to our business operations. One of the assets we evaluated was the Bluetooth software on our laptops, which is used for wireless communication. The system ID for the Bluetooth software is 3, with a CIA asset value of $1000 and a priority rating of medium due to its importance for confidentiality, integrity, and availability. We identified potential threats to this asset, including unauthorized access, interception, and eavesdropping. Hackers could intercept data transmitted over Bluetooth and use it maliciously, posing a significant risk to our business operations. To mitigate these risks, we have put in place controls such as password-protected pairing, disabling discoverability, encryption of data transmitted over Bluetooth, and periodic updates of Bluetooth software and firmware. These controls have an ARO (annual rate of occurrence) of 0.1 and a certainty level of 0.8. Despite these measures, there is still some uncertainty about the effectiveness of our controls, which we have rated at 0.1. Our risk value for this asset is $50.00, which is relatively low. However, we recognize that we could further reduce this risk by avoiding the use of Bluetooth in public places or implementing two-factor authentication for Bluetooth pairing. Our action plan ID is to review our current controls periodically and consider implementing additional measures if necessary. In summary, our overall risk posture is relatively low, but we are constantly evaluating and improving our controls to ensure the security of our assets. Our asset inventory/risk assessment matrix and system/risk assessment matrix provide a visual representation of our assets and the potential risks associated with them, which helps us prioritize our efforts to mitigate those risks.
4. I was a proud owner of a new Apple MacBook in 2020. I used it every day for work, entertainment, and personal tasks. However, I was also aware of the potential risks and vulnerabilities that could compromise the security and availability of my laptop. To conduct an inventory and risk assessment, first listed all my digital and physical assets, including the MacBook. I then categorized the assets based on their type, value, and purpose. Next, I identified the potential threats and vulnerabilities that could affect the MacBook, such as physical theft, unauthorized access, malware and other cyber-attacks, hardware failure, and environmental hazards. I also assessed the likelihood and impact of each threat and vulnerability. Based on my assessment, I prioritized the MacBook as a high-value asset due to its importance for work and personal life. I also valued it at $2500 based on its market price and the value of the data stored on it. To mitigate the risks, I implemented several controls, such as password protection, firewall, encryption, backup and recovery, and physical security measures. I also assessed the uncertainty of these controls and calculated the risk value of the MacBook, which was determined to be moderate. Based on the risk assessment, I identified the need for additional controls, such as regular software and firmware updates, and periodic reviews and updates of the security measures. I estimated the cost of these controls to be $375.00. Overall, I concluded that his risk posture was relatively low, but I recognized the importance of maintaining and updating the controls to prevent any potential security incidents.
5. I had purchased a brand-new Volkswagen SUV in 2018 and was excited to take it out for a spin. But before I did, I knew I needed to assess the risks associated with owning assets. First, I conducted an inventory of all my assets and categorized them based on their purpose. My Volkswagen SUV fell under the category of transportation systems. The vehicle was categorized as a high-value asset, with a CIA (Confidentiality, Integrity, Availability) asset value of $10 million. In identifying potential threats and vulnerabilities to my vehicle, I recognized that it is vulnerable to physical theft, compromise of software, and accidents. In the event of any of these incidents, the confidentiality, integrity, and availability of the vehicle could be compromised, leading to significant financial loss. To mitigate these risks, I have basic security measures in place, such as locking the doors and keeping the vehicle in a secure location when not in use. However, there is still some uncertainty around the effectiveness of these measures, and the likelihood of a threat occurring is rated as medium (.1 ARO). Based on my risk assessment, I determined that there is a significant risk associated with my Volkswagen SUV, with a risk value of $500,000. To reduce this risk, I need to implement additional controls, such as tracking devices and remote access controls, and invest in regular maintenance to ensure the vehicle's software is up-to-date and secure. In conclusion, this risk assessment highlights the need for continuous monitoring and control of assets to mitigate risks associated with them. By identifying vulnerabilities and implementing appropriate controls, we can reduce the likelihood of security incidents and protect our valuable assets.
6. It was a typical afternoon in 2016 when I received a call from the Social Security Administration in Birmingham, Alabama. My heart started racing as I answered the phone, wondering what could be wrong. The representative on the other end of the line informed me that my social security number had been compromised. Someone in California had hacked into my personal information and had attempted to use my social security number to gain employment. My Social Security card was the main asset that was compromised in this incident. It holds a high CIA (Confidentiality, Integrity, Availability) asset value of $100,000, as it contains sensitive personal information that is critical to your financial and reputational well-being. I was shocked and scared. I had always taken great care to protect my social security number, and I couldn't believe that someone had been able to get their hands on it. The representative assured me that they had caught the fraudulent activity and had taken steps to prevent any further misuse of my information. They also provided me with resources and steps to take to protect myself and my identity moving forward. As I hung up the phone, I realized how fortunate I was that the Social Security Administration had caught the fraudulent activity. The potential consequences of having my identity stolen could have been devastating. I immediately went to my desk and pulled out my risk assessment matrix that I had created for my personal assets. My social security card was classified as a high-value asset with a very high-risk value. Given the high value of my social security number and the prevalence of identity theft, I assessed the ARO as "Very High" at 0.2. The confidentiality and integrity of my personal information were at risk, which could lead to financial loss and reputational harm. I had always known that my social security card was an essential asset that required strict controls to prevent unauthorized access. I kept the card in a secure place and never carried it in my wallet. However, I had uncertainty around the effectiveness of these controls, which led to a risk value of $8,000. This incident made me realize that I needed to be even more vigilant in protecting my personal information. I reviewed my asset inventory/risk assessment matrix and my system/risk assessment matrix and identified areas where I needed to improve my controls. I also created an action plan to strengthen my controls and reduce my overall risk posture. In conclusion, this incident taught me the importance of conducting regular risk assessments and maintaining strong controls over high-value assets such as social security cards. With the increasing prevalence of identity theft and cyber-attacks, it's critical to take proactive measures to protect personal information and prevent unauthorized access.
7. My macOS is a critical asset in my inventory, which is used to store sensitive and confidential information. To ensure its security, I assessed its potential risks and vulnerabilities. The inventory was conducted by listing all the critical assets that are essential to your business operations. I categorized your assets by their level of importance, assigning a CIA asset value based on confidentiality, integrity, and availability. I identified threats and vulnerabilities by assessing the potential risks associated with each asset. My macOS, which is used for networking and is essential for my daily business operations, was identified as a high priority asset with a CIA asset value of $500,000. External threats were identified as the primary threat category, and the vulnerability associated with the firewall was identified as a potential point of entry for attackers. To mitigate this vulnerability, controls were already in place, including blocking all incoming traffic except for authorized requests, and the likelihood of an attack was assessed as medium with an ARO of .1. Despite the controls in place, the risk value of this vulnerability was assessed as high with a risk value of $25,000.00, indicating that additional controls may be needed to further reduce risk. The overall risk posture was assessed as moderate, with some areas of concern identified that require additional controls and monitoring.