Practical Assessment: Asset Management

Following your recommendation in the previous module, Oscorp reached out to their internal auditor KPMG to design a 3-year internal audit program to test out cyber security controls.

KPMG conducted their first cyber security internal audit for Oscorp, and a major finding was that the Asset Management process needs further enhancements.

KPMG noted that Oscorp does not have a good handle on asset management. They noted that Oscorp does not have an up to date central asset management database.

Problem:

Oscorp asked you for guidance. They want your advice on how to design a process to capture assets and maintain an up to date CMDB. They currently use a single spreadsheet that has some ad-hoc IT systems details.

Your answer

We need to find the most critical asset We need to assign owner to the asset We need to know how critical the asset it. We need to collaborate with cross-functional teams to find out about that asset.

Apply the following Asset Management recommendations to Oscorp:

- Leverage the current spreadsheet that's used as a CMBD. Use it as a starting point, and further improve it as you go.

- Conduct an asset discovery activity. This can be first accomplished through scanning the network, and comparing the findings with the current list.

- Spend some time with the IT team, validate the current CMDB assets with the IT team. If you find discrepancies, update the CMDB accordingly. The IT team will be a great source to get a list of software and hardware assets from.

- Oscorp is a scientific research organisation. Therefore, you must meet up with stakeholders from various research groups and get a thorough understanding of what research intellectual property each team holds. The "intellectual property" research is the most critical asset for Oscorp.

- Finally, ensure that you meet up with stakeholders from the rest of the business to validate the assets that are documented in the CMDB

- The next step would be to work with the data governance team or the risk team to classify the assets based on sensitivity and criticality.

- The last step is documented a process within the spreadsheet that ensures the CMDB is maintained and is up to date. Recommend that the CMDB is maintained by the IT team. The IT team should have a process to periodically review and validate the CMDB. Depending on how busy the IT team is, a review every 6 to 12 months is usually sufficient.

- Document the roles and responsibility of maintaining the reviewing the CMDB and ensure that senior management endorses and supports the process.

Recommendations:

GRC Mastery by Abed Hamdan