Practical Assessment- TPRM

Oscorp really enjoyed working with you and they decided to extend the contract with your employer. They have a new assignment for you: TPRM.

One of Oscorp's key suppliers is Horizon Labs. They provide Oscorp with a Software-as-a-Service (SaaS) application. Oscorp uses this SaaS application for scientific data analysis.

You are tasked with conducting a security assessment on Horizon Labs as a supplier. You send a TPRM questionnaire to Horizon Labs and they provided you with answers.

We will assume that Horizon Labs provided you with sufficient evidence.

Problem:

Go over the questions and answers and summarise the key risk items that should be escalated to Oscorp's senior management.

Your answer

Horizon Labs is a startup, we still don't follow cyber security frameworks- Cybersecurity frameworks need to be followed for compliance and privacy laws. We don't have a vulnerability scanner but we install regular updates to our windows servers- Vulnerability scan needs to be implemented so we can detect and mitigate vulnerabilities. We haven't done a penetration test yet, but we are plan to run one in the future.- This is needed to know how vulnerable our systems and processes are so we can mitigate risks and minimize company's risks. People are needed for role-based access control, detection and monitoring and to implement the least privileges rule.

There are some obvious high risk items. Here is a summary:

- Horizon Labs don't have a cyber security team or a proper cyber security capability. The IT team manages cyber security. They don't follow a cyber security framework. Therefore, Horizon Labs don't have sufficient cyber security capability which poses a High risk to Oscorp.

- Horizon Labs don't have a vulnerability management program or a penetration testing program. This is another High risk issue.

- Lack of cyber security detection and monitoring capability is a High risk issue.

- Horizon Labs is not capable of responding to cyber security incidents. This is a High risk issue.

- Significant deficiency in the area of Identity and Access Management. This is a high risk issue.

- DLP: Horizon Labs encrypt data and take regular backups. However, they don't monitor for Data loss issues. This a Medium risk. It would be High if they didn't encrypt the data or take backups.

Recommendations:

GRC Mastery by Abed Hamdan