

Practical Assessment: Audit Program



Chief Scientist Harry Osborn has managed to make a breakthrough with his new highly confidential medication.

© Anushka Sinha | github.com/rikusmiles/

Oscorp's CEO asked you to design a cyber security audit program to ensure that Oscorp's cyber security controls are tested on a periodic basis.

Oscorp currently has a small cyber security team that perform various technical activities such as detecting and responding to cyber security incidents and managing the firewalls.

They also have an internal audit function that conducts financial audits.

Problem:

As an external cyber security consultant, how would you design a cyber security audit program for Oscorp using the three lines of defence model?

Your answer

Line-1- Oscorp's own technical team managing the data center devices and networks. Line-2- Oscorp's Line-2 defense to validate line-1's network set up and security controls. Line-3- Oscorp's Line-3 defense to validate Line-2's work and internal audit team to help line-2 to validate what is required.

Following the three lines of defence model, you can propose the following:

- **Line 1:** The cyber security team can perform regular self-audits to ensure that they identify and documents any gaps that they discover.
- **Line 2:** As you've learned in the course, finding individuals who understand GRC and auditing is challenging. You propose that Oscorp hires a full time Cyber Security Auditor to perform Line 2 audits. Bonus points if they hire someone who completed this cyber security GRC Mastery training course!
- **Line 3 (Internal Audit):** Oscorp current internal audit team does not include anyone who can perform cyber security audits (because they're financial auditors). You can propose that Oscorp hires your firm as their internal auditors. Your consulting firm can create an internal audit program for Oscorp that focuses on testing cyber security controls.

Recommendations: © Anushka Sinha | github.com/rikusmiles/
GRC Mastery by Abed Hamdan