

An Introduction to Cyber Assessments

SESSION OUTCOMES

By the end of this course you will have a good grasp of each type of assessment. You will be able to understand better what assessment to use in what circumstance.

SESSION DURATION

2 hours

TARGET AUDIENCE

Designed for employee levels. Recommended for employees in IT teams, internal audit and finance. A useful training for employees in management positions.

CONNECT WITH US

 | [linkedin.com/company/d4n6](https://www.linkedin.com/company/d4n6)

 | /DfourNsixMalta

ABOUT THIS SESSION

Ever wondered on how to measure and test a business resiliency to cyber security? Have you ever assessed the soundness of your company's posture to information security?

There are a number of Cyber Assessments that can be considered for such an exercise. We have designed this course to bridge the gap and provide an understanding to participants on what is the difference between these different assessment types. Here you will learn about:

- Vulnerability Assessments;
- Threat Hunting;
- Penetration Testing;
- Ethical Hacking; and
- IS Auditing.

You will learn how each of these assessments are conducted and what each one entails. You will be able to discern which assessment is most suitable for which outcome.

The course will explore the benefits of each assessment. We will suggested some tools for certain types of assessments and discuss good practices in terms of frequency of application. Moreover you will gain some useful understanding on what is best done in-house and when you should outsource.

CONTACT US

 | +356 7900 8112

 | info@d4n6.com