SISEKELO
Institute of Business & Technology

CYBER SECURITY RISK MANAGEMENT

This course introduces delegates to the key principles of cyber security and its impact on organisational information security systems. It provides delegates with an introduction to risk analysis, risk assessment and risk mitigation for information security systems. In the end, delegates will be provided with tools and templates to use in their company to perform risk assessments.

Who should take this course?

The course is designed for

- IT professionals, such as Practitioners, responsible for managing cyber risk strategy
- General risk managers who would like to improve their knowledge of cyber risk.
- General Managers who are keen on improving their knowledge of cyber risk

Learning outcomes

At the end of the programme, delegates will be able to;

- Understand the basic principles of cyber security
- Understand how cyber-attacks are executed and the negative impact thereof
- Demonstrating an understanding of business processes and potential cyber risks to a unit.
- Identifying potential cyber risks and assessing the impact thereof in a unit.
- Developing contingency plans for managing risk.
- Testing and revising contingency plans.

Introduction to Cybersecurity

- What is Cybersecurity
- Why cybersecurity is becoming increasingly important
- What can be done to defend your business from cyber-crimes
- Overview of tools and techniques leveraged by leading businesses to defend their data

Understand Potential Cyber risks to a business

- Explain the concept of risk with reference to cyber risk
- Identify and explain the factors that could constitute cyber risks to a unit
- Outline the different types of cyber risks
- Explain the role of organisational policies and procedures in relation to risk management
- The impact of cyber threats

Identifying, assessing the impact and dealing with Risk

- Identify and document potential risk factors for critical processes in a unit
- Identify and document possible scenarios that could constitute a risk a
- Evaluate and record the possibility of each scenario occurring for future use
- Perform and document an analysis to rate the impact of each scenario on a unit
- Determine the priorities resulting from the impact analysis and document it for implementation in the event of the risk materialising

Develop contingency plans for managing cyber risk

- Develop and document contingency plans in accordance with the entity's cyber security management policies and procedures
- Communicate contingency plans to relevant stakeholders in accordance with the entity's risk management procedures
- Distribute contingency plans and store it in accordance with the entity's risk management procedures

Test and revise contingency plans

- Test contingency plans in accordance with the entity's cyber risk management procedures
- Document recommendations on improvements to the contingency plans in relation to the findings of the testing
- Revise contingency plans to incorporate recommendations from the testing in accordance with the entity's policies and procedures

Pricing and payment terms (as per schedule)

- R10 500.00
- Alternative payment terms must be discussed and agreed upon before course commencement.
- Valid Purchase Order numbers accepted.

Duration

Course is available for 3 days.

Delivery Mode

- 100% online
- Instructor led sessions
- Access to recorded sessions
- Self-paced learning
- Online assessments

SISEKELO
Institute of Business & Technology
ACCELERATING POTENTIAL

CONTACT INFO

Unit 6C2 Sinosteel Plaza
159 Rivonia Road Morningside Ext 39, Sandton
011 666 6000
info@sisekelo.co.za