CATALYST.AI

E: info@apexu.co.za
T: 011 568 6629
apexu.co.za

SHORT

Accredited Skills Programme:

ADVANCED CYBER SECURITY

NQF Level 5

TOTAL CREDITS: 10

DURATION
3 Months

A: 54 Wierda Road, St Andrews, Ground Floor, Wierda Valley, Sandton
Campus A: Block M, Central Park, 400 16th Rd, Randjespark, Midrand, 1685

CATALYST.AI

apexu.co.za

PROGRAMME OVERVIEW

The Advanced Cybersecurity Skills Programme has been meticulously crafted to empower participants with advanced cybersecurity skills and knowledge, positioning them as a proficient leader within the cybersecurity domain. Throughout the programme, participants will explore a diverse range of topics and concepts, each strategically designed to enhance their capabilities in the evolving landscape of cybersecurity.

This skills programme is underpinned by:

SAQA ID	Title	Credits
12891	Apply concepts and principles of business ethics in the professional environment	5
13107	Develop understanding within an organisation about the risks associated with its functioning and context	5

ENTRY REQUIREMENTS

To enrol in the Advanced Cybersecurity skills programme, participants must meet the following entry requirements:

- Communication at NQF Level 5.
- Computer Literacy at NQF Level 5.
- Knowledge of IT infrastructure and risks associated with it.

LEARNING OUTCOMES

By the end of this programme, participants will:

1. Showcase comprehension of cybersecurity ethics, encompassing fundamental concepts and principles.
2. Apply professional judgment in navigating practical cybersecurity scenarios, making informed and ethical decisions.
3. Implement ethical procedures within the cybersecurity domain, ensuring a professional and morally sound environment.
4. Offer guidance on cybersecurity strategies, processes, and capabilities, considering the contextual dynamics influencing the organisation's security posture.
5. Profile the organisation's cybersecurity risk philosophy, understanding its stance and approach toward managing cybersecurity risks and advise on the cybersecurity risk management strategies of the organisation, ensuring a proactive and resilient cybersecurity posture.
6. Provide expert counsel on aligning the organisation's cybersecurity risk management philosophies with effective implementation strategies.

PROGRAMME STRUCTURE

Module1 – Showcase comprehension of cybersecurity ethics, encompassing fundamental concepts and principles

- Concepts and principles relating to business ethics
- Exploring the Philosophy and Framework of Cybersecurity Ethics
- Understanding Cybersecurity Ethics

Module 2 – Apply professional judgement in navigating practical cybersecurity scenarios, making informed and ethical decisions

- Meaning of professional judgment and its application

Module 3 – Implement ethical procedures within the cybersecurity domain, ensuring a professional and

morally sound environment

- What is workplace ethics?
- Basic principles to help you make ethical decisions

Module 4 – Offer guidance on cybersecurity strategies, processes, and capabilities, considering the contextual dynamics influencing the organisation's security posture

- Cybersecurity Strategy Essentials
- Key Components of a Strategic Cybersecurity Plan

Module 5 – Profile the organisation's cybersecurity risk philosophy, understanding its stance and approach toward managing cybersecurity risks and advise on the cybersecurity risk management strategies of the organisation, ensuring a proactive and resilient cybersecurity posture

- Introduction to Compliance and Governance
- Key Concepts in Regulatory Compliance and Governance

Module 6 – Provide expert counsel on aligning the organisation's cybersecurity risk management philosophies with effective implementation strategies

- Introduction to Continuous Monitoring
- Tools and Techniques for Effective Monitoring

ASSESSMENT

- Formative and Summative Assessment: Continuous evaluation through theoretical and practical assessments.