

OCCUPATIONAL QUALIFICATION

Cybersecurity Analyst

Level 5 | SAQA ID – 118986



Edge Training is a proudly Level 1 B-BBEE accredited skills training provider with a national footprint and full accreditation with QCTO and SETA partners. We remain aligned with evolving QCTO regulations, ensuring that skills development in South Africa continues to meet national standards. Our commitment to compliance, excellence and quality assurance reinforces our role in strengthening the national framework and contributing meaningfully to the advancement and sustainability of skills development training.

Table of Contents

Qualification Information	03
Edge Training Will Provide	07
Qualification Structure	08
Additional Information	09

Qualification Information

Occupational Qualification: Cybersecurity Analyst

Level 5

SAQA ID – 118986

173 Credits

Entry Requirements:

- NQF Level 4

Occupational Purpose:

Cybersecurity Analysts apply the practice of protecting assets such as networks, computer systems and information assets from malicious attacks and threats. They assess and mitigate risks and potential intrusions and identify risks and vulnerabilities. They study existing techniques for managing security issues and maintaining the security of information and systems in the working environment ensuring legal compliance

Occupational Tasks:

- Demonstrate knowledge and understanding of cybersecurity concepts and investigate how cybersecurity affects legal compliance and solidarity in companies and communities (NQF Level 5)
- Assess risk to assets and evaluate current cybersecurity protection measures (NQF Level 5)
- Implement detection, protection and prevention systems and respond to breaches or incidences (NQF Level 5)

Qualification Information

Purpose of the Knowledge Modules:

The knowledge acquired will enable learners to demonstrate an understanding of:

(KM-01):

- The fundamentals of various computer and network security threats such as identity theft, credit card fraud, phishing, virus and backdoors, emails hoaxes, loss of confidential information, hacking attacks, and social engineering

(KM-02):

- The principles and techniques applied in the editing and proofreading processes
Network Security and Defence

(KM-03):

- The principles of cybersecurity and Ethical Hacking and the types of threats and attacks and the respective risk

(KM-04)

- The various legislations governing the workplace and their implication for the employer and employees
- Areas of performance management, business planning concepts, costing of products and concepts of general ethical behaviour and its impact in the workplace

(KM-05):

- The design thinking principles and application in the workplace

(KM-06):

- Acquire mathematical thinking theory for solving problems and acquire basic maths knowledge for using software toolkits or platforms

(KM-07)

- Understanding of what computers can do, the processes that make them function in terms of: the input, output, CPU (central processing unit), and memory
- It gives an overview of networks and connectivity

(KM-08)

- Data and databases and giving meaning to data through data processing, analysis and visualisation

Qualification Information

Purpose of the Knowledge Modules:

The knowledge acquired will enable learners to demonstrate an understanding of:

(KM-09):

- 4IR on communities, individuals and businesses and important skills for future needs

Purpose of the Practical Modules:

The focus of the learning in the practical modules is on providing the learner an opportunity to:

(PM-01):

- Participate in organisational governance ensuring all systems are put in place to achieve compliance with legal requirements and nationally accepted standards
- Configure computers and mobile devices to connect to networks and to the internet

(PM-02):

- Acquire the skills to assess risks, vulnerabilities and trends and evaluate current security measures and security posture of an organisation

(PM-03):

- Protect all company data, particularly sensitive data, from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability

(PM-04):

- Use basic maths as a basis for understanding maths encountered in the programming within the field of networking

(PM-05):

- Apply basic scripting skills to use a toolsets in the field of study or employment

(PM-06):

- Acquire the skills to analyse and visualise data

(PM-07):

- Participate in a design thinking intervention and apply design thinking methodologies and look for opportunities to apply the same methodology in world-of-work and personal life

Qualification Information

Purpose of the Practical Modules:

The knowledge acquired will enable learners to demonstrate an understanding of:

(PM-08):

- Acquire the skills to function ethically and effectively in the workplace

Purpose of the Workplace Modules:

The focus of the work experience module is on providing the learner an opportunity to:

(WM-01):

- Demonstrate knowledge and understanding of cybersecurity concepts and investigate how cybersecurity affects legal compliance and solidarity in companies and communities

(WM-02):

- Assess risk to assets and evaluate current cybersecurity protection measures

(WM-03):

- Conduct a cybersecurity risk assessment under supervision and apply detection, protection and prevention processes

Edge Training Will Provide

- Full project management of qualification
- Registration of the qualification with the relevant SETA
- Enrolment of the learner with QCTO for the qualification
- Facilitation by a Subject Matter Expert
- Venue suitable for the number of delegates
- Course material
- Monthly progress reports via the Edge Client Portal
- Booking of final exam (EISA) with the relevant SETA
- Certificates of Attendance

Qualification Structure

Cybersecurity Analyst | Total Credits: 173

	Knowledge Modules	Level	Credits
KM01	Introduction to Cybersecurity	4	8
KM02	Fundamentals of Network Security and Defence (Network Defender)	5	12
KM03	Cybersecurity and Cyber Threats and Attacks (Ethical Hacking)	5	12
KM04	Introduction to Cybersecurity Governance, Legislation and Ethics	4	4
KM05	Fundamentals of Design Thinking and Innovation	4	1
KM06	Refresher: Logical Thinking and Basic Calculations	4	3
KM07	Computers, Devices and Computing Systems	4	6
KM08	Data and Databases Vulnerabilities	4	3
KM09	Introduction to 4IR and Future Skills	4	4

Knowledge Modules | Total Credits: 53

	Practical Modules	Level	Credits
PM01	Ensure Compliance in terms of Legal Cybersecurity Requirements and National and International Standards	5	4
PM02	Assess Risks and Vulnerabilities and Evaluate Current Security Measures	5	20
PM03	Implement Protection, Prevention and Detection Measures to Mitigate Risk, Violations and Vulnerabilities	5	20
PM04	Apply Logical Thinking and Maths: Refresher	4	6
PM05	Apply Basic Scriptwriting for Cybersecurity Toolsets	4	4
PM06	Access and Visualise Structured Data Using Spreadsheets: Refresher	4	5
PM07	Applying Design Thinking Methodologies	4	4
PM08	Function Ethically and Effectively as a Member of a Multidisciplinary Team	4	5

Practical Modules | Total Credits: 68

	Workplace Modules	Level	Credits
WM01	Compliance with Legal Cybersecurity Requirements	5	12
WM02	Cybersecurity Risk Assessment and Mitigation	5	20
WM03	Cybersecurity Detection, Protection and Prevention Processes	5	20

Work Experience Modules | Total Credits: 52

Additional Information

Alternative titles used by the industry:

- None

Get in Touch

 087 135 5543  www.edgetraining.co.za  info@edgetraining.co.za

We are a fully accredited training provider with BEE Level 1 certification and SSETA Accreditation #1135. Our VAT number is 4640189041, and we are registered under the number 2017 / 349079 / 07.