OCCUPATIONAL CERTIFICATE: **CYBERSECURITY ANALYST**

NQF 5

(173 credits)

QUALIFICATION OVERVIEW

The purpose of this qualification is to prepare learners to operate as Cybersecurity Analysts. 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 also study existing techniques for managing security issues and maintaining the security of information and systems in the working environment, ensuring legal compliance.

A qualified learner will be able to:

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

DURATION

18 Months.

WHO SHOULD ATTEND

The programme is intended for individuals that are existing employees who have experience in this field, but without formal recognition of skills and competencies.

It is also intended for individuals who wish to extend their careers into Security Architect, Security Engineer and Cybersecurity auditor.

OCCUPATIONAL CERTIFICATE: CYBERSECURITY ANALYST NQF 5

PREREQUISITES

We offer a thorough pre-assessment process to align learners to appropriate qualifications and levels. Entry requirements for this qualification include:

- NQF Level 4 qualification

DELIVERY METHOD

Face-To-Face / Virtual Training

CONTACT

To enrol your Learners or for more information, please contact your Business Development Consultant on 0861 ILEARN or email info@ilearn.co.za.

LEARNING OUTCOMES

Knowledge Modules

- Introduction to Cybersecurity.
- Fundamentals of Network Security and Defence (Network Defender).
- Cybersecurity and Cyber Threats and Attacks (Ethical Hacking).
- Introduction to Cybersecurity Governance, Legislation and Ethics.
- Fundamentals of Design Thinking and Innovation.
- Refresher: Logical Thinking and Basic Calculations.
- Computers, Devices and Computing Systems.
- Data and Databases Vulnerabilities.
- Introduction to 4IR and Future Skills.

Practical Modules

- Ensure Compliance in terms of Legal Cybersecurity Requirements and National and International Standards.
- Assess Risks and Vulnerabilities and Evaluate Current Security Measures.
- Implement Protection, Prevention and Detection Measures to Mitigate Risk.
- Violations and Vulnerabilities.
- Apply Logical Thinking and Math's: Refresher.
- Apply Basic Scriptwriting for Cybersecurity Toolsets.
- Access and Visualise Structured Data Using Spreadsheets: Refresher.
- Applying Design Thinking Methodologies.
- Function Ethically and Effectively as a Member of a Multidisciplinary Team.

LEARNING OUTCOMES

Workplace Module

- Compliance with Legal Cybersecurity Requirements
- Cybersecurity Risk Assessment and Mitigation
- Cybersecurity Detection, Protection and Prevention Processes

OCCUPATIONAL CERTIFICATE: CYBERSECURITY ANALYST NQF 5

PROJECT PLAN - SAQA: 118986

Exit Level Outcome	Type	Module Numbers	Clusters	NQF	Credit	Training Session Dates
Qualification Induction						
Cluster 1: Cybersecurity and 4IR Fundamentals						
ELO 1: Analyse, identify, and solve potential and actual security risks, vulnerabilities and inefficiencies to safeguard information system assets from malicious cybersecurity attacks.	Knowledge Module	252901001-KM-01	Introduction to Cybersecurity	4	8	4 Days (Month 1)
	Knowledge Module	252901001-KM-09	Introduction to 4IR and Future Skills	4	4	2 Days (Month 2)
Cluster 1: Feedback and Remediation - Cybersecurity and 4IR Fundamentals						**1 Day**
Cluster 2: Cybersecurity Ethics and Compliance						
ELO 3: Execute ethical cybersecurity monitoring in line with cybersecurity policies to provide defence to a level of confidentiality, integrity, and availability equal with the threat to assets and their value to the company. ELO 4: Execute response procedures to mitigate cyber-attacks and secure information assets, intellectual property, and computer systems.	Knowledge Module	252901001-KM-04	Introduction to Cybersecurity Governance, Legislation and Ethics	4	4	4 Days (Month 3)
	Practical Module	252901001-PM-01	Ensure Compliance in terms of Legal Cybersecurity Requirements and National and International Standards	5	4	
Cluster 2: Feedback and Remediation - Cybersecurity Ethics and Compliance						**1 Day**
Workplace _Logbook Submission		**252901001-WM-01**	**Compliance with Legal Cybersecurity Requirements**	**5**	**12**	**Month 4**
Cluster 3: Network Security Essentials						
ELO 1: Analyse, identify, and solve potential and actual security risks, vulnerabilities and inefficiencies to safeguard information system assets from malicious cybersecurity attacks. ELO 2: Protect organisation's digital assets from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability. ELO 4: Execute response procedures to mitigate cyber-attacks and secure information assets, intellectual property, and computer systems.	Knowledge Module	252901001-KM-02	Fundamentals of Network Security and Defense (Network Defender)	5	12	5 Days (Month 4)
	Practical Module	252901001-PM-03	Implement Protection, Prevention and Detection Measures to Mitigate Risk, Violations and Vulnerabilities	5	20	7 Days (Month 5)
Cluster 3: Feedback and Remediation - Network Security Essentials						**1 Day**
Workplace _Logbook Submission		**252901001-WM-03**	**Cybersecurity Detection, Protection and Prevention Processes**	**5**	**20**	**Month 6**

OCCUPATIONAL CERTIFICATE: CYBERSECURITY ANALYST NQF 5

PROJECT PLAN - SAQA: 118986

Exit Level Outcome	Type	Module Numbers	Clusters	NQF	Credit	Training Session Dates
Qualification Induction						
Cluster 4: Cybersecurity tools						
ELO 2: Protect organisation's digital assets from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability	Knowledge Module	252901001-KM-03	Cybersecurity and Cyber Threats and Attacks (Ethical Hacking)	4	12	5 Days (Month 6)
ELO 4: Execute response procedures to mitigate cyber-attacks and secure information assets, intellectual property, and computer systems.	Practical Module	252901001-PM-05	Apply Basic Scriptwriting for Cybersecurity Toolsets	4	4	2 Days (Month 7)
Cluster 4: Feedback and Remediation - Cybersecurity tools						**1 Day**
Cluster 5: Design Thinking for Recovery Protocols						
ELO 5: Execute recovery protocols and procedures as per recovery plan to restore data and/or assets affected by cybersecurity incidents.	Knowledge Module	252901001-KM-05	Fundamentals of Design Thinking and Innovation	4	1	3 Days (Month 8)
	Practical Module	252901001-PM-07	Applying Design Thinking Methodologies	4	4	
Cluster 5: Feedback and Remediation - Design Thinking for Recovery Protocols						**1 Day**
Cluster 6: Logical Thinking Numeracy						
ELO 3: Execute ethical cybersecurity monitoring in line with cybersecurity policies to provide defence to a level of confidentiality, integrity, and availability equal with the threat to assets and their value to the company.	Knowledge Module	252901001-KM-06	Refresher: Logical Thinking and Basic Calculations	4	3	4 Days (Month 9)
	Practical Module	252901001-PM-04	Apply Logical Thinking and Maths: Refresher	4	6	
Cluster 6: Feedback and Remediation - Logical Thinking Numeracy						**1 Day**
Cluster 7: Data Access and Security						
ELO 2: Protect organisation's digital assets from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability.	Practical Module	252901001-PM-06	Access and Visualise Structured Data Using Spreadsheets: Refresher	4	5	3 Days (Month 10)
Cluster 7: Feedback and Remediation - Data Access and Security						**1 Day**

OCCUPATIONAL CERTIFICATE: CYBERSECURITY ANALYST NQF 5

PROJECT PLAN - SAQA: 118986

Exit Level Outcome	Type	Module Numbers	Clusters	NQF	Credit	Training Session Dates
Qualification Induction						
Cluster 8: Computer Systems						
ELO 4: Execute response procedures to mitigate cyber-attacks and secure information assets, intellectual property, and computer systems.	Knowledge Module	252901001-KM-07	Computers, Devices and Computing Systems	4	6	3 Days (Month 11)
Cluster 8: Feedback and Remediation - Computer Systems						**1 Day**
Cluster 9: Database Security and Risk Assessment						
ELO 1: Analyse, identify, and solve potential and actual security risks, vulnerabilities and inefficiencies to safeguard information system assets from malicious cybersecurity attacks.	Knowledge Module	252901001-KM-08	Data and Databases Vulnerabilities	4	3	2 Days (Month 12)
ELO 2: Protect organisation's digital assets from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability.	Practical Module	252901001-PM-02	Assess Risks and Vulnerabilities and Evaluate Current Security Measures	5	20	7 Days (Month 13)
Cluster 9: Feedback and Remediation - Database Security and Risk Assessment						**1 Day**
Workplace _Logbook Submission		**252901001-WM-02**	**Cybersecurity Risk Assessment and Mitigation**	**5**	**20**	**Month 14**
Cluster 10: Team Ethics						
ELO 3: Execute ethical cybersecurity monitoring in line with cybersecurity policies to provide defense to a level of confidentiality, integrity, and availability equal with the threat to assets and their value to the company.	Practical Module	252901001-PM-08	Function Ethically and Effectively as a Member of a Multidisciplinary Team	4	5	3 Days (Month 14)
Cluster 10: Team Ethics						**1 Day**

FINAL REMEDIATION	1 Day (Month 15)	
MOCK EXAM	1 Day (Month 15)	
EXTERNAL INTEGRATED SUMMATIVE ASSESSMENT (EISA)	1 Day	
PREPARATION FOR EISA RE-WRITE	1 Day	
EXTERNAL INTEGRATED SUMMATIVE ASSESSMENT (EISA) - SECOND ATTEMPT	1 Day	