SOUTH AFRICAN QUALIFICATIONS AUTHORITY

REGISTERED QUALIFICATION THAT HAS PASSED THE END DATE:

Occupational Certificate: Cybersecurity Analyst

SAQA QUAL ID	QUALIFICATION TITLE			
118986	Occupational Certificate: Cybersecurity Analyst			
ORIGINATOR				
Development Quality Partner-MICT SETA				
PRIMARY OR DELEGATED QUALITY ASSURANCE FUNCTIONARY			**NQF SUB-FRAMEWORK**	
-			OQSF - Occupational Qualifications Sub-framework	
QUALIFICATION TYPE	**FIELD**		**SUBFIELD**	
Occupational Certificate	Field 10 - Physical, Mathematical, Computer and Life Sciences		Information Technology and Computer Sciences	
ABET BAND	**MINIMUM CREDITS**	**PRE-2009 NQF LEVEL**	**NQF LEVEL**	**QUAL CLASS**
Undefined	173	Not Applicable	NQF Level 05	Regular-Provider-ELOAC
REGISTRATION STATUS		**SAQA DECISION NUMBER**	**REGISTRATION START DATE**	**REGISTRATION END DATE**
Passed the End Date - Status was "Registered"		EXCO 0522/24	2022-04-21	2025-12-31
LAST DATE FOR ENROLMENT		**LAST DATE FOR ACHIEVEMENT**		
2026-12-31		2029-12-31		

In all of the tables in this document, both the pre-2009 NQF Level and the NQF Level is shown. In the text (purpose statements, qualification rules, etc), any references to NQF Levels are to the pre-2009 levels unless specifically stated otherwise.

This qualification does not replace any other qualification and is not replaced by any other qualification.

PURPOSE AND RATIONALE OF THE QUALIFICATION

Purpose:
The purpose of this qualification is to prepare a learner to operate as a Cybersecurity Analyst.

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.

On completion of this qualification, the learner will be able to demonstrate an understanding of and how to investigate cybersecurity issues and challenges as they affect the legal compliance, communities, society, the ICT sector, and the economy. The learner will understand how cybercrime can affect businesses causing disruption, how to respond effectively to incidences such as vulnerabilities testing and threats and how to analyse their consequences. The learner also evaluates efficient design of efficient security solutions and ensures 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.

Rationale:
As Information and Communication Technology (ICT) adoption rates increase so does cybercrime and, in direct relation, the serious need for security and integrity of ICT systems is recognised as being of paramount importance. The urgent need and demand for competent personnel have been increasing over time.

There is a global shortage of cybersecurity experts, and this number is diminishing every year. The recently published 2019 (ISC) 2 Cybersecurity Workforce Study pointed to a severe shortage of cybersecurity professionals. The study estimated, for the first time, that there are 2.8 million skilled professionals worldwide currently working in the field and that an additional 4.07 million more are needed to defend organizations. Acquiring this qualification will assist in fulfilling the obvious and serious need for cyber security experts, will have a direct, positive impact on the ICT sector and will consequently benefit the economy as well.

The global cybersecurity market size is forecasted to grow to ZAR 3764 billion by 2023. In Africa the cyber security market size grows from ZAR 14 billion in 2015 to ZAR35 Billion by 2020, at a Compound Annual Growth Rate (CAGR) of 20.41% from 2015 to 2020. According to 6Wresearch, South Africa's Cyber Security Market size is projected to register a CAGR of 11.1% during 2020-26.

There are no similar qualifications registered on the NQF other than those used as articulation possibilities in the section below and no professional registration or licencing is expected for Cybersecurity Analysts to seek employment in the sector.

Through the growth of Cyber Security Analysts that have completed this qualification, it is expected that there will be a measurable reduction in Cyber Crime-related disruption in business continuity, a reduction in losses incurred and an increase in the number of perpetrators brought to justice. It will also provide a remedy to the severe shortage of cybersecurity professionals in Africa.

Cybersecurity Analysts can be employed as Cybersecurity Specialists, Information Security Specialists, Security Analysts, Cyber Monitoring Analysts, Security Consultants or Network Security Analysts.

Typical learners include school leavers, graduates from TVET colleges and those currently in employment without formal recognition of competencies.

This qualification will support the recommendations of the Presidential Commission on the 4th Industrial Revolution. This recommendations forefront human capital and the future of work and refers to growing skills instability. It states that work will change, and that robotic process automation (RPA) will play a more pivotal role in the execution of tasks. The 4th Industrial Revolution (4IR) is a fusion of advances in artificial intelligence (AI), robotics, process automation, the Internet of Things (IoT), genetic engineering, quantum computing, cyber security, cloud computing and data science.

LEARNING ASSUMED TO BE IN PLACE AND RECOGNITION OF PRIOR LEARNING

Recognition of Prior Learning (RPL):
RPL for Access to the Qualification
- Learners will gain access to the qualification through RPL for Access as provided for in the QCTO RPL Policy. RPL for access is conducted by accredited education institution, skills development provider or is workplace accredited to offer that specific qualification/part qualification.
- Learners who have acquired competencies of the modules of a qualification or part qualification will be credited for modules through RPL.

RPL for Access to the External Integrated Summative Assessment
Accredited providers and approved workplaces must apply the internal assessment criteria specified in the related curriculum document to establish and confirm prior learning. Accredited providers and workplaces must confirm prior learning by issuing a statement of result.

Entry Requirements:
The minimum entry requirement for this qualification is:
- NQF Level 4 qualification.

RECOGNISE PREVIOUS LEARNING?

Y

QUALIFICATION RULES

This qualification is made up of compulsory Knowledge, Practical Skill and Work Experience Modules:

Knowledge Modules
- 252901-001-00-KM-01 Introduction to Cybersecurity, Level 4, 8 Credits.
- 252901-001-00-KM-02 Fundamentals of Network Security and Defence, Level 5, 12 Credits.
- 252901-001-00-KM-03 Cybersecurity and Cyber Threats and Attacks, Level 5, 12 Credits.
- 252901-001-00-KM-04 Introduction to Cybersecurity Governance, Legislation and Ethics Level 4, 4 Credits.
- 252901-001-00-KM-05 Fundamentals of Design Thinking and Innovation, Level 4, 1 Credit.
- 252901-001-00-KM-06 Logical Thinking and Basic Calculations, Level 4, 3 Credits.
- 252901-001-00-KM-07 Computers, Devices and Computing Systems, Level 4, 6 Credits.
- 252901-001-00-KM-08 Data and Database Vulnerabilities, Level 4, 3 Credits.

- 252901-001-00-KM-09 Introduction to 4IR and Future Skills, Level 4, 4 Credits.

Total number of credits for Knowledge Modules: 53

Practical Skill Modules
- 252901-001-00-PM-01 Ensure Compliance in terms of Legal Cybersecurity Requirements and National and International Standards, Level 5, 4 Credits.
- 252901-001-00-PM-02 Assess Risks and Vulnerabilities and Current Security Measures, Level 5, 20 Credits.
- 252901-001-00-PM-03 Implement Protection, Prevention and Detection Measures to Mitigate Risk, Violations and Vulnerabilities, Level 5, 20 Credits.
- 252901-001-00-PM-04 Apply Logical Thinking and Maths, Level 4, 6 Credits.
- 252901-001-00-PM-05 Apply Basic Scriptwriting for Cybersecurity Toolsets, Level 4, 4 Credits.
- 252901-001-00-PM-06 Access and Visualise Structured Data Using Spreadsheets, Level 4, 5 Credits.
- 252901-001-00-PM-07 Apply Design Thinking Methodologies, Level 4, 4 Credits.
- 252901-001-00-PM-08 Function Ethically and Effectively as a Member of a Multidisciplinary Team, Level 4, 5 Credits.

Total number of credits for Practical Skill Modules: 68

Work Experience Modules
- 252901-001-00-WM-01 Compliance with Legal Cybersecurity Requirements, Level 5, 12 Credits.
- 252901-001-00-WM-02 Cybersecurity Risk Assessment and Mitigation, Level 5, 20 Credits.
- 252901-001-00-WM-03 Cybersecurity Detection, Protection and Prevention Processes, Level 5, 20 Credits.

Total number of credits for Work Experience Modules: 52

EXIT LEVEL OUTCOMES

1. Analyse, identify, and solve potential and actual security risks, vulnerabilities and inefficiencies to safeguard information system assets from malicious cybersecurity attacks.
2. Protect organisation's digital assets from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability.
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.
4. Execute response procedures to mitigate cyber-attacks and secure information assets, intellectual property, and computer systems.
5. Execute recovery protocols and procedures as per recovery plan to restore data and/or assets affected by cybersecurity incidents.

ASSOCIATED ASSESSMENT CRITERIA

Associated Assessment Criteria for Exit Level Outcome 1:
- Perform regular checks to ensure security practices are compliant with organisational policies and security requirements as well as the legal and regulatory requirements.
- Identify critical systems, and critical Information System Assets.
- Conduct vulnerability testing to identify weaknesses, vulnerabilities and risks in hardware, software and information technology (IT) infrastructures.
- Collect and leverage data on current security measures for risk analysis and write regular system status reports.
- Identify the optimum method of securing the IT infrastructure and Information Systems Assets of an organisation.
- Maintain and check risk catalogue against incidence reports on a scheduled basis.

Associated Assessment Criteria for Exit Level Outcome 2:
- Analyse and implement anti-virus systems, firewalls, data centres and software defensive protocol updates with a security-first mindset.
- Safeguard information system assets by identifying and solving potential and actual security problems.
- Grant credentials to authorized users, monitor access-related activities and do checks for unregistered information changes.
- Implement security improvements by analysing current situation, evaluating trends, and performing risks and threat analysis.
- Implement and automate Intruder Detection and Prevention Systems and associated response protocols.

Associated Assessment Criteria for Exit Level Outcome 3:
- Apply security monitoring and incident response toolsets to detect and trace intrusions and test the environment with a focus on continuous improvement.
- Report detected incidences by identifying and analysing abnormalities and violations.
- Detect security vulnerabilities and inefficiencies by conducting periodic checks and tests and collaborate with cybersecurity team to update defensive protocols as necessary.
- Demonstrate a comprehensive understanding of ethics and a moral compass as applicable to cybersecurity.

Associated Assessment Criteria for Exit Level Outcome 4:
- Monitor and respond to unusual activities and attacks, implement appropriate defensive protocols if breaches occur, and report incidents.
- Perform response and mitigation activities to close off the security vulnerability, prevent expansion of an event and to resolve the incident.
- Collect data on current security measures for risk analysis and write regular system status reports.

- Execute investigations into network intrusions and other cyber security breaches.

Associated Assessment Criteria for Exit Level Outcome 5:
- Find the means of security breach immediately and quarantine the corrupted servers, devices and systems to prevent spreading and to protect against additional vulnerabilities.
- Identify information that was lost/stolen, analyse its impact and start remediation procedures.
- Analyse attacks and develop cybersecurity improvements based on lessons learned from such attacks as well as reviews of existing measures.
- Produce an incident close-out report with appropriate logs and other substantiating evidence.

Integrated Assessment:
Integrated Formative Assessment
The skills development provider will use the curriculum to guide them on the stipulated internal assessment criteria and weighting. They will also apply the scope of practical skills and applied knowledge as stipulated by the internal assessment criteria. This formative assessment together with work experience leads to entrance in the integrated external summative assessment.

Integrated summative assessment
An external integrated summative assessment, conducted through the relevant QCTO Assessment Quality partner is required for the issuing of this qualification. The external integrated summative assessment will focus on the exit level outcomes and associated assessment criteria.

The external integrated summative assessment will be conducted through a theoretical assessment and the evaluation of practical tasks at decentralised approved assessment sites in a simulated environment and conducted by an assessor(s) registered with the relevant AQP.

INTERNATIONAL COMPARABILITY

The Occupational Certificate: Cybersecurity Analyst was compared with the British Level 5 Diploma in Cyber Security and a sequence of programs leading to CompTIA exams and certifications. CompTIA operates globally.

United Kingdom:
The London School of International Business offers a Level 5 Diploma in Cyber Security. The method of presentation is a blended approach and includes online study, study material, e-library availability and tutor support via live chat or email. It has 120 credits and is advertised as a self-paced learning experience over a period of 9 months. Entry requirements are stated as Level 4 Award/Diploma.

Learning outcomes are:
- Understand key cryptographic principles and modes.
- Understand the standards, regulations and laws that apply to business and government organisations in relation to encryption.
- Understand the core principles of digital investigations.
- Apply the types of tools that support professional digital investigations at a strategic level.
- Apply Business Continuity Management to major incident planning and response.
- Evaluate the management streams and performance monitoring mechanisms that relate to information security.
- Understand how data protection legislation impacts considerations of strategy-setting and strategic leadership.
- Understand the physical and human resources required to manage a major suspected cyber security incident.
- Understand the role of senior leaders and strategic leadership.
- Plan for investigations and forensics teams.

Mandatory units include:
- Cryptography.
- Digital Investigations and Forensics.
- Communications and Incident Management.
- Strategic Leadership.

Similarities:
Both qualifications are at Level 5 and the entry requirement is Level 4. Content related to the above-mentioned learning outcomes 1 - 8 is similar in both qualifications.

Differences:
Content related to the above-mentioned learning outcomes 9 and 10 is not included in the Occupational Certificate: Cybersecurity Analyst.

United States of America (USA):
A second comparability was conducted against best of practice which is with a sequence of modules leading to Computing Technology Industry Association (CompTIA) certifications, namely IT Fundamentals+, A+, Network+ and Security+. The successful completion of these modules in the sequence captured leads to a CompTIA certification. The duration of these modules is not specified, other than that it is self-paced and offered online by a number of institutions, such as Pearson Education. CompTIA is the leading provider of vendor-neutral IT certifications in the world.

The content of this sequence of courses include:
IT Fundamentals+ includes the following aspects: Identify and explain the basics of computing, IT infrastructure, application and software, software development, database fundamentals and security, as well as install software, establish basic network connectivity, identify/prevent basic security risks, explain troubleshooting theory and

preventative maintenance of devices.

A+ includes the following aspects: Baseline security topics core to the IT support role, including physical versus logical security concepts and measures, malware, competency in operational procedures including basic disaster prevention and recovery and scripting basics, dependency on networking and device connectivity as well as demonstrate baseline security skills for IT support professionals, configure device operating systems, troubleshoot and problem solve core service and support challenges while applying best practices for documentation, change management, and scripting, support basic IT infrastructure and networking, configure and support PC, mobile and IoT device hardware, Implement basic data backup and recovery methods and apply data storage and management best practices.

Network+ includes the following aspects: Identify benefits and drawbacks of existing network configurations, implement network security, standards, and protocols, troubleshoot network problems, support the creation of virtualized networks

Security+ includes the following aspects: Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions, help identify attacks and vulnerabilities to mitigate them before they infiltrate, understand secure virtualization, secure application deployment, and automation concepts, identify and implement the best protocols and encryption, understand the importance of compliance, awareness of applicable laws and policies, including principles of governance, risk, and compliance

Similarities
The OC: Cybersecurity Analyst entails all the above content aspects. In terms of the CompTIA courses, lab tasks and capstone projects provide for the practical skills component which can be regarded as similar to the practical skills component in the OC: Cybersecurity Analyst.

Differences
The duration of the OC: Cybersecurity Analyst is specified as 11 months whilst the CompTIA modules are a number of consecutive short modules. The OC: Cybersecurity Analyst includes learning in the workplace.

Conclusion
This South African qualification compares favourably with the competencies covered in the international qualifications and programmes.

ARTICULATION OPTIONS

This qualification provides opportunities for horizontal and vertical articulation options.

Horizontal Articulation:
- Higher Certificate in Computer Forensics, NQF Level 05.

Vertical Articulation:
- Advanced Certificate in Information Security, NQF Level 06.

NOTES

Qualifying for External Assessment:
To qualify for an external assessment, learners must provide proof of completion of all required knowledge and practical modules by means of statements of results and a record of completed work experience.

Additional Legal or Physical Entry Requirements:
- None.

Criteria for the accreditation of providers
Accreditation of providers will be done against the criteria as reflected in the relevant curriculum on the QCTO website.

The curriculum title and code are: Cybersecurity Analyst: 252901-001-00.

Encompassed Trade:
This qualification encompasses the following trades as recorded on the NLRD:
- This is not a trade qualification.

Assessment Quality Partner (AQP)
- MICT SETA.

LEARNING PROGRAMMES RECORDED AGAINST THIS QUALIFICATION:

NONE

PROVIDERS CURRENTLY ACCREDITED TO OFFER THIS QUALIFICATION:

This information shows the current accreditations (i.e. those not past their accreditation end dates), and is the most complete record available to SAQA as of today. Some Primary or Delegated Quality Assurance Functionaries have a lag in their recording systems for provider accreditation, in turn leading to a lag in notifying SAQA of all the providers that they have accredited to offer qualifications and unit standards, as well as any extensions to accreditation end dates. The relevant Primary or Delegated Quality Assurance Functionary

should be notified if a record appears to be missing from here.

NONE
