IMPACTFUL
Powered by LRMG

ASSESSMENT QUALITY PARTNER
mictseta

IT LEARNERSHIPS

CYBERSECURITY ANALYST

QUALIFICATION 118986
LEARNERSHIP Q-NUMBER: 32Q320181231735

Build cybersecurity capability that protects organisations

As organisations become more digital, the risk of cyber threats continues to grow. Strong cybersecurity capability is critical to protecting systems, data, and operations.

This Cybersecurity Analyst learnership builds practical capability to identify risks, monitor threats, and implement security measures. Learners develop the skills to protect systems and respond to security incidents effectively.

Whether your learners are starting out, moving into IT, or looking to specialise in a high-demand field, this qualification opens the door to roles like Cybersecurity Analyst, Security Operations Analyst, or Information Security Practitioner.

QCTO

On successful completion of this qualification, learners are awarded: **Occupational Certificate: Cybersecurity Analyst (SAQA ID: 118986)**

We work closely with you to understand your objectives, guide you through the requirements, and support the implementation of qualifications that deliver real impact.

NQF LEVEL **5**

CREDITS **173**

WHO SHOULD ENROL?

- Organisations strengthening cybersecurity and risk capability
- Teams responsible for IT security and data protection
- Individuals starting a career in software development or AI
- School leavers interested in coding and intelligent technologies
- Professionals looking to move into AI or machine learning roles

WHAT MAKES THIS COURSE DIFFERENT?

This qualification is designed to move you from learning to doing

- Build strong foundations in cybersecurity principles, risk management, and threat detection
- Apply your skills in practical, hands-on environments that simulate real security scenarios
- Gain experience monitoring systems, identifying vulnerabilities, and responding to security threats

WHAT IS THE ENTRY CRITERIA?

- Grade 12

IMPACTFUL
Powered by LRMG

ASSESSMENT QUALITY PARTNER
mictseta

CYBERSECURITY ANALYST

QUALIFICATION

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.

Skills your team will build

These skill level outcomes show what you'll be able to do in practice:

- 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)

Recognised, quality-assured qualification

Learners undergo internal assessment across the knowledge, practical, and workplace modules, all of which are formally assessed and moderated, in line with QCTO requirements. Successful completion of all components ensures that learners are EISA-ready for the External Integrated Summative Assessment.

To obtain the qualification, learners must pass the External Integrated Summative Assessment (EISA), conducted at an Accredited Assessment centre under the oversight of an Assessment Quality Partner (AQP). The EISA evaluates learners' competence against the qualification's Exit Level Outcomes through integrated written, practical, and/or work-based assessment methods, in line with approved external assessment specifications.

Let's partner for impact!

Our approach combines a deep understanding of your objectives with expert guidance on QCTO programmes, ensuring smooth implementation and meaningful impact in the workplace.

We'll help you get clear on the holistic implementation process

From first conversation to final assessment, you'll be supported by a team that understands how to make QCTO qualifications work in practice.

Delivered your way

- Classroom | Johannesburg
- Virtual | Instructor-led
- On-site | Nationwide

Contact us to start your journey!

impactful@lrmg.co.za
impactful.co.za

An environment that enables your learning journey

To ensure a successful learning journey, you need to be supported by the right tools, systems and experienced mentors in a structured environment that workplace standards. Everything is designed to help you learn, practice and perform with confidence.

Physical Requirements

- Tools, equipment, systems, e.g.: company systems, documents, data, relevant meetings, teams and supervisors, design studio, etc.
- Key processes, e.g.: CYBERSECURITY design, testing and deployment processes project on the go or completed

Human Resource Requirements

- Maximum mentor/learner ratio of 1:3 in the ideal situation.
- Supervisor/mentor: 2 years' software development experience

Legal Requirements

- Legal (product) licences to use software.
- OHS compliance certificate.
- Ethical clearance (where necessary)

CYBERSECURITY ANALYST

QUALIFICATION

This detailed overview outlines how the qualification is structured to develop capability progressively – from foundational knowledge, through applied practical skills, to integrated workplace experience. Each module is aligned to the credit requirements of the nationally recognised qualification

KNOWLEDGE MODULES (53 CREDITS)

ID	Name	Level	Credits
252901-001-00-KM-01	**Introduction to Cybersecurity**	**4**	**8**
The main focus of the learning in this knowledge module is to build an understanding of 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 The learning will enable learners to demonstrate an understanding of:			
KM-01-KT01	Introduction to computer and mobile device security		
KM-01-KT02	Various computer and network security threats		
KM-01-KT03	Identity theft		
KM-01-KT04	Adopting good cybersecurity practices		
KM-01-KT05	Safeguard mobile, media and social networking profiles as user		
KM-01-KT06	Protecting computers, accounts and data as user		
KM-01-KT07	Understand security incidents and reporting		

ID	Name	Level	Credits
252901-001-00-KM-02	**Fundamentals of Network Security and Defence (Network Defender)**	**5**	**12**
The main focus of the learning in this knowledge module is to build an understanding of the principles and techniques applied in the editing and proofreading processes network security and defence The learning will enable learners to demonstrate an understanding of:			
KM-02-KT01	Introduction to network security		
KM-02-KT02	Network risk and vulnerability management		
KM-02-KT03	Network defence fundamentals		
KM-02-KT04	Monitoring for breaches and attacks		
KM-02-KT05	Network incident response and management		

ID	Name	Level	Credits
252901-001-00-KM-03	**Cybersecurity and Cyber Threats and Attacks (Ethical Hacking)**	**5**	**12**
The main focus of the learning in this knowledge module is to build an understanding of principles of cybersecurity and Ethical Hacking and the types of threats and attacks and the respective risk. The learning will enable learners to demonstrate an understanding of:			
KM-03-KT01	Information security Governance and compliance		
KM-03-KT02	Information security		
KM-03-KT03	Footprinting and Reconnaissance		
KM-03-KT04	Scanning Networks		
KM-03-KT05	Enumeration		
KM-03-KT06	Vulnerability Analysis		
KM-03-KT07	System Hacking		
KM-03-KT08	Malware Threats		
KM-03-KT09	Sniffing		
KM-03-KT10	Social Engineering		
KM-03-KT11	Denial-of-Service		
KM-03-KT12	Session Hijacking		
KM-03-KT13	Evading IDS, Firewalls, and Honeypots		
KM-03-KT14	Hacking Web Servers		
KM-03-KT15	SQL Injection		
KM-03-KT16	Hacking Wireless Networks		
KM-03-KT17	Hacking Mobile Platforms		
KM-03-KT18	IoT Hacking		
KM-03-KT19	Cloud Computing		
KM-03-KT20	Cryptography		
KM-03-KT21	Cyber incident response and management		

ID	Name	Level	Credits
252901-001-00-KM-04	**Introduction to Cybersecurity Governance, Legislation and Ethics**	**4**	**4**
The main focus of the learning in this knowledge module is to acquire general knowledge and understanding of the various legislations governing the workplace and their implication for the employer and employees. The learning of this module will also enable the learner to acquire an understanding of the principles of areas of performance management, business planning concepts, costing of products and concepts of general ethical behaviour and its impact in the workplace The learning will enable learners to demonstrate an understanding of:			
KM-04-KT01	Governance		
KM-04-KT02	Legislation governing workplaces		
KM-04-KT03	Introduction to ethics and security		
KM-04-KT04	Ethics at work		
KM-04-KT05	Security		
KM-04-KT06	Performance management		
KM-04-KT07	Business planning		
KM-04-KT08	Costing of products		
KM-04-KT09	Resources		

ID	Name	Level	Credits
252901-001-00-KM-05	Fundamentals of Design Thinking and Innovation	4	1
The main focus of the learning in this knowledge module is to build an understanding of the design thinking principles and application in the workplace The learning will enable learners to demonstrate an understanding of:			
KM-05-KT01	Introduction to design thinking		
KM-05-KT02	The human element		
KM-05-KT03	Creativity		
KM-05-KT04	Innovation		
KM-05-KT05	Design		
KM-05-KT06	Design thinking methodology		
KM-05-KT07	Application of design thinking		

ID	Name	Level	Credits
252901-001-00-KM-06	Refresher: Logical Thinking and Basic Calculations	4	3
The main focus of the learning in this knowledge module is to acquire mathematical thinking theory for solving problems and acquire basic maths knowledge for using software toolkits or platforms The learning will enable learners to demonstrate an understanding of:			
KM-06-KT01	Mathematical thinking skills for problem solving.		
KM-06-KT02	Basic math		
KM-06-KT03	Conversion between decimal and binary systems		
KM-06-KT04	Express size and magnitude		
KM-06-KT05	Error in calculations		
KM-06-KT06	Cartesian coordinate system		
KM-06-KT07	Pythagorean theorem for finding the distance between two points		
KM-06-KT08	Operator precedence		
KM-06-KT09	Integer division		
KM-06-KT10	Modulus		
KM-06-KT11	Increments		

ID	Name	Level	Credits
252901-001-00-KM-07	**Computers, Devices and Computing Systems**	**4**	**6**
The main focus of the learning in this knowledge module is to build an understanding of what computers can do, and the processes that make them function in terms of the four major parts: the input, output, CPU (central processing unit), and memory. It gives an overview of networks and connectivity The learning will enable learners to demonstrate an understanding of:			
KM-07-KT01	Problem solving skills for IT Professionals		
KM-07-KT02	Techniques for safety		
KM-07-KT03	System components		
KM-07-KT04	Motherboards		
KM-07-KT05	Processors		
KM-07-KT06	Memory		
KM-07-KT07	BIOS and CMOS		
KM-07-KT08	Hard drives and storage devices		
KM-07-KT09	Power supplies and voltage		
KM-07-KT10	Ports, cables, and connectors		
KM-07-KT11	Input and output devices		
KM-07-KT12	Installing and managing printers		
KM-07-KT13	Mobile devices, multimedia, and laptop computers		
KM-07-KT14	Preventative maintenance		
KM-07-KT15	Troubleshooting procedures		
KM-07-KT16	Operating systems		
KM-07-KT17	Managing files		
KM-07-KT18	Applications utility, troubleshooting, and optimization		
KM-07-KT19	Configuring device drivers		
KM-07-KT20	Networking and wireless connections		
KM-07-KT21	Recovery		
KM-07-KT22	Cloud computing		
KM-07-KT23	Security fundamentals		
KM-07-KT24	Introduction to applications		

ID	Name	Level	Credits
252901-001-00-KM-08	**Data and Databases Vulnerabilities**	**4**	**3**
The main focus of the learning in this knowledge module is to build an understanding of data and databases and giving meaning to data through data processing, analysis and visualisation The learning will enable learners to demonstrate an understanding of:			
KM-08-KT01	Data vulnerability and security		
KM-08-KT02	Data and data processing		
KM-08-KT03	Databases, data storage and access to data		
KM-08-KT04	Structured query language (SQL)		
KM-08-KT05	Data scraping		
KM-08-KT06	Software for analysing and visualising data		

ID	Name	Level	Credits
252901-001-00-KM-09	**Introduction to 4IR and Future Skills**	**4**	**4**
The main focus of the learning in this knowledge module is to build an understanding of the impact of 4IR on communities, individuals and businesses and important skills for future needs The learning will enable learners to demonstrate an understanding of:			
KM-09-KT01	4 IR emerging trends		
KM-09-KT02	Computing Knowledge		
KM-09-KT03	Future skills and competencies (4IR)		
KM-09-KT04	4 IR trends affecting businesses		
KM-09-KT05	Interpersonal skills		
KM-09-KT06	Intrapersonal skills		
KM-09-KT07	Communication principles and methods		
KM-09-KT08	Written business communication		
KM-09-KT09	Presentation skills		
KM-09-KT10	Teamwork in the workplace		
KM-09-KT11	Committees and meetings		
KM-09-KT09	Job descriptions and profiles		
KM-09-KT13	Customers and stakeholders		
KM-09-KT14	Customer service		

PRACTICAL SKILL MODULES (68 CREDITS)

ID	Name	Level	Credits
252901-001-00-PM-01	**Ensure Compliance in terms of Legal Cybersecurity Requirements and National and International Standards**	**5**	**4**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to participate in organisational governance ensuring all systems are put in place to achieve compliance with legal requirements and nationally accepted standards. In addition they will acquire skills to configure computers and mobile devices to connect to networks and to the internet The learner will be required to:			
PM-01-PS01	Ensure compliance of computer systems, networks and data with legal cybersecurity requirements and national and international standards		
PM-01-PS02	Apply basic computing and IT infrastructure procedures to ensure secure computer use		
PM-01-PS03	Set up computer systems and networks applying applicable cybersecurity protocols		
PM-01-PS04	Protect, detect, and respond to network attacks as first line defence		
Associated Knowledge Module: KM-02 Fundamentals of Network Security and Defence			

ID	Name	Level	Credits
252901-001-00-PM-02	**Assess Risks and Vulnerabilities and Evaluate Current Security Measures**	**5**	**20**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to assess risks, vulnerabilities and trends and evaluate current security measures and security posture of an organisation The learner will be required to:			
PM-02-PS01	Apply and use functions of a suitable toolset for cybersecurity purposes		
PM-02-PS02	Scan systems for and identify vulnerabilities and potential security threats to information systems and analyse their consequences		
PM-02-PS03	Evaluate the level of risk in an IT system using standard security models and apply appropriate countermeasures		
PM-02-PS04	Use appropriate tools to assess the security posture of an organisation		
Associated Knowledge Module: KM-03 Cybersecurity and Cyber Threats and Attacks (Ethical Hacking),			

ID	Name	Level	Credits
252901-001-00-PM-03	**Implement Protection, Prevention and Detection Measures to Mitigate Risk, Violations and Vulnerabilities**	**5**	**20**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to protect all company data, particularly sensitive data, from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability The learner will be required to:			
PM-03-PS01	Protect all company data, particularly sensitive data, from both internal and external threats		
PM-03-PS02	Provide security monitoring in alignment with cybersecurity's mission to protect digital assets to a level of confidentiality, integrity and availability equal with the threat to those assets and their value to the organisation (Prevent, monitor, maintain)		
PM-03-PS03	Detect warning signs which may indicate security breaches		
PM-03-PS04	Assist with incidence response in case of a cybersecurity violations		
PM-03-PS05	Understand and comply with the disaster recovery plan		
PM-03-PS06	Effectively respond to security incidents by detecting and identification		
PM-03-PS07	Act immediately to mitigate the impact of an incident		
PM-03-PS08	Execute measures to remediate cybersecurity incidents		
PM-03-PS09	Execute measures to recover from cybersecurity incidents		
PM-03-PS10	Assess and learn lessons from the event ensuring continuous improvement		
Associated Knowledge Module: KM-03 Cybersecurity and Cyber Threats and Attacks (Ethical Hacking),			

ID	Name	Level	Credits
252901-001-00-PM-04	**Apply Logical Thinking and Maths**	**4**	**6**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to use basic maths as a basis for understanding maths encountered in the programming within the field of networking The learner will be required to:			
PM-04-PS01	Number bases and measurement units		
PM-04-PS02	Basic math		
PM-04-PS03	Operator precedence		
PM-04-PS04	Integer division		
PM-04-PS05	Modulus		
PM-04-PS06	Increments		
Associated Knowledge Module: KM-06 Refresher Logical Thinking and Basic Calculations,			

ID	Name	Level	Credits
252901-001-00-PM-05	**Apply Basic Scriptwriting for Cybersecurity Toolsets**	**4**	**4**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to apply basic scripting skills to use a toolset in the field of study or employment The learner will be required to:			
PM-05-PS01	Source and compare at least three software toolkits/platforms/ languages used in your field of studies		
PM-05-PS02	Set up an editing environment (tailored to a specific tool or platform)		
PM-05-PS03	Write a script using a Command Line Interface/Terminal session for giving instructions for use of a toolset		
PM-05-PS04	Script write loops (tailored to a specific tool or platform)		
PM-05-PS05	Handle errors (tailored to a specific tool or platform)		
PM-05-PS06	Apply general steps for writing script (tailored to a specific tool or platform)		
PM-05-PS07	Practical exercise using the specified product set		
Associated Knowledge Module: KM-03 Cybersecurity and Cyber Threats and Attacks (Ethical Hacking)			

ID	Name	Level	Credits
252901-001-00-PM-06	**Access and Visualize Structured Data Using Spreadsheets**	**4**	**5**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to analyse and visualise data The learner will be required to:			
PM-06-PS01	Report data		
PM-06-PS02	Summarise and format data using tables		
PM-06-PS03	Create, use and edit pivot tables and pivot charts		
PM-06-PS04	Create, use and edit dashboards		
PM-06-PS05	Create and configure hierarchies and time data		
PM-06-PS06	Apply a data model		
PM-06-PS07	Import data from files		
PM-06-PS08	Import data from databases		
PM-06-PS09	Import data from reports		
PM-06-PS10	Visualize data		

ID	Name	Level	Credits
252901-001-00-PM-07	**Applying Design Thinking Methodologies**	**4**	**4**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to 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 The learner will be required to:			
PM-07-PS01	Collaborate with team members to apply innovative and problem-solving strategies.		
PM-07-PS02	Apply design thinking process to solve a problem creatively and innovatively		
Associated Knowledge Module: KM-05 Fundamentals of Design Thinking and Innovation			

ID	Name	Level	Credits
252901-001-00-PM-08	**Function Ethically and Effectively as a Member of a Multidisciplinary Team**	**4**	**5**
The focus of the learning in this module is on providing the learner with an opportunity to acquire the skills to function ethically and effectively in the workplace The learner will be required to:			
PM-08-PS01	Present information to an audience		
PM-08-PS02	Conduct basic research (gather and explore data and information) on 4IR skills and application opportunities in the workplace		
PM-08-PS03	Ensure compliance with the code of conduct and governance in the workplace		
PM-08-PS04	Collaborate with team members in the workplace		
PM-08-PS05	Attend and participate in meetings		
Associated Knowledge Module: KM-09 Introduction to 4IR and Future Skills			

WORK EXPERIENCE MODULES (52 CREDITS)

ID	Name	Level	Credits
252901-001-00-WM-01	**Compliance with Legal Cybersecurity Requirements**	**5**	**12**
The focus of the work experience is on providing the learner with an opportunity to: Demonstrate knowledge and understanding of cybersecurity concepts and investigate how cybersecurity affects legal compliance and solidarity in companies and communities The learner will be required to:			
WM-01-WE01	Attend induction program and familiarise self with company processes, procedures, tools and culture • Attend induction program and familiarise self with the culture of the company. • Apply protocols and work etiquette. • Attend company specific information sharing sessions (e.g. standing meetings, toolbox talks, power hours, etc.) • Familiarise self with and apply "working from anywhere" protocols. • Read and understand company cybersecurity policy, protocols and procedures. • Comply with governance protocols and code of ethics of the company and ensure legal compliance by adhering to legal requirements (incl. but not limited to privacy, confidentiality, security of data, etc.). • Spend time in the various departments of the company, observe process flows and compile wire diagrams or workflow of the processes observed using suitable tools and showing the relationships and influences each of the departments have on each other. • Understand management requirements and expectations from cybersecurity measures. • Understand cybersecurity protocols and procedures. • Understand company assets in terms of cybersecurity. • Manage timesheets and apply self-management skills. • Collaborate with team members to achieve common and individual goals		
WM-01-WE02	Shadow and observe an experienced Cybersecurity Analyst undertaking the following tasks • Comply with requirements of risk management frameworks • Comply with security regulations and standards • Monitor compliance with information security policies and procedures • Give advice and guidance to staff on issues such as spam and unwanted or malicious emails. • Train organisation on security measures • Maintain an information security risk register and assist with internal and external audits relating to information security • Administering information security software and controls • Maintaining security records of monitoring and incident response activities • Document security breaches and assess the damage they cause. • Producing situational and incident-related reports • Providing timely and relevant security reports • Generate reports for both technical and non-technical staff and stakeholders		

ID	Name	Level	Credits
252901-001-00-WM-01	**Compliance with Legal Cybersecurity Requirements**	**5**	**12**
WM-01-WE03	Conduct the following tasks under supervision • Comply with requirements of risk management frameworks • Comply with security regulations and standards • Monitor compliance with information security policies and procedures • Give advice and guidance to staff on issues such as spam and unwanted or malicious emails. • Train organisation on security measures • Maintain an information security risk register and assist with internal and external audits relating to information security • Administering information security software and controls • Maintaining security records of monitoring and incident response activities • Document security breaches and assess the damage they cause. • Producing situational and incident-related reports • Providing timely and relevant security reports • Generate reports for both technical and non-technical staff and stakeholders		

ID	Name	Level	Credits
252901-001-00-WM-02	**Cybersecurity Risk Assessment and Mitigation**	**5**	**20**
The focus of the work experience is on providing the learner with an opportunity to: Assess risk to assets and evaluate current cybersecurity protection measures The learner will be required to:			
WM-02-WE01	Shadow and observe an experienced Cybersecurity Analyst undertaking a cybersecurity risk assessment • Determine information value • Identify and prioritise assets • Identify cyber threats • Identify vulnerabilities • Analyse controls and the need for new controls • Calculate the likelihood and impact of various scenarios on a per-year basis • Prioritize risks based on the cost of prevention vs information value • Document results in risk assessment report		
WM-02-WE02	Conduct a cybersecurity risk assessment under supervision • Determine information value • Identify and prioritise assets • Identify cyber threats • Identify vulnerabilities • Analyse controls and the need for new controls • Calculate the likelihood and impact of various scenarios on a per-year basis • Prioritize risks based on the cost of prevention vs information value • Document results in risk assessment report		

ID	Name	Level	Credits
252901-001-00-WM-03	**Cybersecurity Detection, Protection and Prevention Processes**	**5**	**20**
The focus of the work experience is on providing the learner with an opportunity to: Conduct a cybersecurity risk assessment under supervision and apply detection, protection and prevention processes. The learner will be required to:			
WM-03-WE01	Shadow and observe an experienced Cybersecurity Analyst undertaking the following tasks • Protect • Prevent • Detect • Respond and recover		
WM-03-WE02	Conduct a cybersecurity risk assessment under supervision • Protect • Prevent • Detect • Respond and recover		