SECTION A:	QUALIFICATION DETAILS																	
QUALIFICATION DEVELOPER (S)	**NEW ERA COLLEGE OF ARTS, SCIENCE AND TECHNOLOGY**																	
TITLE	Bachelor of Science in Cyber Security and Risk Management													**NCQF LEVEL**	7			
STRANDS (where applicable)	N/A																	
FIELD	Information and Communication Technology													**CREDIT VALUE**	505			
SUB FIELD	Information Technology																	
New Qualification			Legacy Qualification											Renewal Qualification	√			
														Registration Code	QO240			
SUB-FRAMEWORK	General Education			TVET				Higher Education	√									
QUALIFICATION TYPE	Certificate	I		II		III		IV		V		Diploma		Bachelor	√			
	Bachelor Honours			Post Graduate Certificate				Post Graduate Diploma										
	Masters			Doctorate/ PhD														

RATIONALE AND PURPOSE OF THE QUALIFICATION

The introduction of the Bachelor of Science in Cyber Security and Risk Management is justified by the increasing threat of cybercrime and the shortage of skilled cyber security professionals in Botswana and the wider SADC region. As government, private institutions, and critical services continue to rely heavily on ICT systems, the risk of cyber-attacks, data breaches, fraud, and other computer-related crimes has become a major national concern.

The Government of Botswana has prioritised crime reduction, cybercrime prevention, safety, and risk management through national frameworks such as the National Development Plan, Vision 2036, and the Cybercrime and Computer Related Crimes Act of 2018. These initiatives highlight the need for qualified professionals who can support law enforcement, protect digital systems, manage organisational risks, and contribute to national security.

This programme will prepare graduates with the knowledge and practical skills required to prevent, detect, investigate, and respond to cyber threats. It will also equip them to advise public and private organisations on risk management strategies that support institutional stability, security, and achievement of organisational goals.

The programme is further justified by the growing demand for cyber security expertise in areas such as digital governance, financial services, law enforcement, education, telecommunications, and public administration. By producing graduates in cyber security and risk management, the College will contribute to national capacity building, strengthen Botswana's response to cybercrime, and support regional skills development. The programme is also expected to attract students from Botswana, the SADC region, and beyond due to the limited availability of similar qualifications in the region.

PURPOSE: (itemise exit level outcomes)

The purpose of the qualification is to produce graduates with specialized knowledge, skills, and competence to:

1. **Analyse** cyber security threats, vulnerabilities, and risks within public, private, financial, and non-financial organisational environments.
2. **Apply** cyber security principles, tools, and techniques to prevent, detect, respond to, and manage cybercrime and computer-related incidents.
3. **Evaluate** organisational risk management practices and recommend appropriate controls to support secure and resilient operations.
4. **Implement** international best practices, legal requirements, ethical standards, and governance frameworks in cyber security and risk management contexts.
5. **Conduct** research and use evidence-based approaches to solve complex cyber security and risk management problems locally, regionally, and internationally.
6. **Demonstrate** professional competence, critical thinking, communication, teamwork, and leadership skills required for employability and global competitiveness in the cyber security and risk management field.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

The minimum entry requirements for the Bachelor of Science in Cyber Security and Risk Management program, including provisions for access and inclusion, are detailed below:

Full-time Entry Requirements

The standard entry requirement for the full-time program is specified as:

- Certificate IV (NCQF level 4) with 6 subjects and passes in English, Mathematics, and two Science subjects or equivalent.

Access and Inclusion Mechanisms

Applicants who do not meet the standard academic criteria may still be considered for access through specific policies, demonstrating the program's commitment to inclusion:

- Recognition of Prior Learning (RPL): Applicants who do not meet the Certificate IV criteria but possess relevant industry experience may be considered for access through RPL policies.
- Credit Accumulation and Transfer (CAT): Consideration for access is also provided through Credit Accumulation and Transfer (CAT) policies.

The consideration of applicants through RPL and CAT policies will adhere to guidelines set by the NEC Academic Regulations which are aligned with BQA/National policies. Candidates utilizing RPL and CATS must meet the necessary criteria established by NEC in accordance with the Botswana Qualifications Authority (BQA) respective policies and regulations.

(Note: Please use Arial 11 font for completing the template)

SECTION B	**QUALIFICATION SPECIFICATION**
GRADUATE PROFILE (LEARNING OUTCOMES) **By the end of the programme, learners should be able to:**	**ASSESSMENT CRITERIA**
1. **Identify** common cyber security threats, vulnerabilities, and attack methods in organisational information systems.	1.1 Common cyber security threats are correctly identified. 1.2 System vulnerabilities are described in relation to organisational information systems. 1.3 Different attack methods are explained using relevant examples. 1.4 The possible impact of threats and vulnerabilities on organisations is outlined.
2. **Explain** the principles of cyber security, risk management, information assurance, and digital governance in public and private sector contexts.	2.1 Key cyber security principles are clearly explained.

	2.2 Risk management concepts are described accurately. 2.3 Information assurance principles are linked to data protection and system security. 2.4 Digital governance concepts are explained in relation to organisational operations.
3. **Use** appropriate cyber security tools and techniques to detect, prevent, and respond to computer-related security incidents.	3.1 Appropriate tools are selected for specific cyber security tasks. 3.2 Security techniques are correctly applied to detect and prevent threats. 3.3 Incident response procedures are demonstrated in a practical or simulated environment. 3.4 Tool results are interpreted accurately and reported clearly.
4. **Assess** organisational risk exposure and propose suitable controls to reduce security, operational, and compliance risks.	4.1 Organisational risks are identified and categorised. 4.2 The likelihood and impact of risks are assessed. 4.3 Suitable controls are recommended to reduce identified risks. 4.4 Proposed controls are justified in relation to organisational needs and compliance requirements.
5. Interpret relevant cybercrime laws, ethical requirements, standards, and governance frameworks applicable to cyber security practice.	5.1 Relevant cybercrime laws and regulations are identified. 5.2 Ethical issues in cyber security practice are explained. 5.3 Applicable standards and governance frameworks are interpreted correctly. 5.4 Legal and ethical requirements are applied to practical cyber security scenarios.
6. **Develop** basic cyber security and risk management plans for protecting organisational systems, data, and digital assets.	6.1 Key assets, threats, and risks are identified in the plan. 6.2 Appropriate security measures and risk controls are included. 6.3 Roles, responsibilities, and response procedures are clearly outlined.

	6.4 The plan is practical, structured, and aligned with organisational security needs.
7. Carry out research on cyber security and risk management issues using appropriate methods, data, and academic sources.	7.1 A relevant cyber security or risk management problem is clearly defined. 7.2 Appropriate research methods are selected and applied. 7.3 Relevant data and academic sources are used to support the research. 7.4 Findings are analysed and presented in a logical and evidence-based manner.
8. Present cyber security and risk management findings clearly through reports, presentations, and professional communication.	8.1 Findings are organised clearly and logically. 8.2 Reports follow appropriate academic or professional formats. 8.3 Presentations communicate key information effectively. 8.4 Technical information is explained clearly for the intended audience.
9. Work effectively in teams to solve practical cyber security and risk management problems.	9.1 Team roles and responsibilities are carried out effectively. 9.2 Collaboration and communication within the team are demonstrated. 9.3 Contributions support the achievement of the group task. 9.4 Practical solutions are developed through teamwork and shared decision-making.
10. Demonstrate professional conduct, ethical judgement, and responsibility when handling information security and risk-related tasks.	10.1 Professional behaviour is demonstrated during practical and academic tasks. 10.2 Ethical judgement is applied when handling sensitive information. 10.3 Confidentiality, integrity, and accountability are observed. 10.4 Tasks are completed responsibly and in line with cyber security practice standards.

Note: Please use Arial 11 font for completing the template)

SECTION C	QUALIFICATION STRUCTURE				
COMPONENT	TITLE	Credits Per Relevant NCQF Level			Total Credits
		Level [6]	Level [7]	Level [8]	480
FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Communication and Technical Writing	10			10
	Introduction to computer	15			15
	Cybercrime protection and Society	10			10
	Fundamentals of Information System security & Mgt.	10			10
	Computer System Architecture	10			10
	Operating Systems Concepts	15			15
	Discrete Mathematics for computing	10			10
CORE COMPONENT Subjects/Courses/ Modules/Units	Computer Networks		15		15
	Introduction to Python Programming		15		15
	Network, Internet and System security		15		15
	Security strategies in windows and Linux platforms		15		15
	Database fundamentals		15		15
	Auditing IT Infrastructures for Compliance		10		10

	Foundations of Risk Management in Cybersecurity	10			10
	Cyber Security Project Management		10		10
	Wireless and mobile communication security		15		15
	Legal, Regulatory, and Ethical Issues in Risk Management		10		10
	Research Methods		10		10
	Ethical Hacking		15		15
	Industry Based Learning			50	50
	Individual Project in Cyber Security			15	15
	Cryptography and Data Protection		15		15
	Cyber Threats and Attack Vectors	15			15
	Business Continuity and Disaster Recovery Management		10		10
	Entrepreneurship			10	10
	Social Engineering and Cyber Attack		15		15
	C Programming		15		15
	Cloud Computing		15		15
	Internet of Things (IoT) devices Cyber security and Risk Management		15		15
	Incident Response for Cyber		15		15

	AI for Cyber Security & Digital Forensics		15		15
	Digital Forensics and Investigation		15		15
ELECTIVE COMPONENT Subjects/Courses/ Modules/Units (**CHOOSE FOUR ELECTIVES**)	Strategic Technology Management and Innovation		10		10
	Information Systems Audit and Control		10		10
	Cyber Security Emerging Technologies and Trends		10		10
	AI safety, governance, and risk assessment		10		10
	Front-End Web Development		15		15
	JavaScript		15		15
	C# Programming		15		15
	Natural language processing for spam and phishing defence		15		15
	AI-based biometric authentication and anomaly detection		15		15
STRANDS/ SPECIALIZATION	Subjects/ Courses/ Modules/Units	**Credits Per Relevant NCQF Level**			**Total Credits**
		Level [6]	**Level [7]**	**Level [8]**	

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	**Credit Value**
6	**105**
7	**325**
8	**75**
TOTAL CREDITS	**505**

Rules of Combination:

(Please Indicate combinations for the different constituent components of the qualification)

Component definitions

- Fundamental component: Communication, basic computing and foundational topics that underpin the qualification outcomes (listed Fundamental modules).
- Core component: Essential technical, management and applied cybersecurity modules including capstone(s) and workplace learning.
- Elective component: Specialist or emerging-topic modules. Students choose four electives unless the programme board approves otherwise.

Mandatory combination rules (the minimum for an award)

1. All Fundamental modules must be attempted and passed (i.e., the Fundamental component is mandatory).
2. All Core modules are mandatory unless explicitly identified as elective or unless a formal substitution/RPL is approved by the Programme Board.
3. Electives: Select exactly four elective modules (total elective credits in the model = 55).
4. Project & Industry Based Learning: Completion of Industrial Based Learning (50 credits) and the Individual Project (15 credits) at Level 8 is mandatory for the award. These cannot be replaced by simple classroom modules.

Awarding and transcript rules

- **To receive the qualification award, the candidate must:**
    1. Pass all Fundamental modules;
    2. Pass all Core modules (unless substituted/RPL approved);
    3. Pass two electives; and
    4. Complete Industrial Based Learning (50) and Individual Project (15).

Subtotals by NCQF Level

NCQF Level	Total Credits
Fundamentals modules	**80**
Core modules	**375**
Electives (Choose 4 Modules)	**50**
Grand Total	**505**

(Note: Please use Arial 11 font for completing the template)

ASSESSMENT ARRANGEMENTS

All assessments, formative and summative, leading/contributing to the award of credits or a qualification should be based on learning outcomes and/or sub-outcomes.

Summative assessment

The Final Examination contributes to 60% of the final grade.

Formative assessment

Formative assessments contribute to 40% of the final grade.

MODERATION ARRANGEMENTS

Moderation Arrangements

Assessment and moderation for this qualification shall be conducted in accordance with the Education and Training Provider's (ETP) approved Assessment and Moderation Policy, which is fully aligned with the Botswana Qualifications Authority (BQA) and relevant National Assessment and Moderation Frameworks.

The ETP will ensure that:

1. **All assessments** (formative, summative) are conducted by BQA-accredited assessors who are competent and approved to assess against the registered unit standards or modules within this qualification.
2. **Internal moderation** is systematically implemented to verify that assessment instruments, processes, and decisions are valid, reliable, consistent, and meet national quality standards.
3. **External moderation** is undertaken by BQA-accredited moderators to ensure that assessment outcomes are credible and that national standards are maintained across all assessment sites and delivery modes.
4. Moderation shall be both pre-assessment (verification of assessment tools and marking guides) and post-assessment (verification of sample scripts).
5. The ETP maintains records of all assessment and moderation activities, including assessor and moderator registration details, moderation reports, and evidence of corrective actions implemented where applicable.
6. The moderation process will ensure that learners are fairly, consistently, and transparently assessed in accordance with the learning outcomes and NCQF level descriptors.

RECOGNITION OF PRIOR LEARNING

Candidates may be granted access to the qualification, exemptions, or credit transfer through the application of the ETP's Recognition of Prior Learning (RPL) and Credit Accumulation and Transfer (CAT) policies, in line with national policies. However, the full qualification shall not be awarded solely through RPL. RPL may be used to recognise relevant prior learning and experience for entry, module exemption, or credit towards the qualification, subject to assessment and approval by the

relevant academic structures. Candidates must complete the required minimum credits and meet the exit level outcomes of the qualification before the award can be granted.

CREDIT ACCUMULATION AND TRANSFER

The Credit Accumulation and Transfer (CAT) policy shall apply to this qualification in line with institutional and national requirements. Through CAT, candidates may be granted credit transfer for relevant and equivalent modules or learning already completed at a recognised institution. However, the full qualification shall not be awarded solely through CAT. Candidates must complete the required minimum institutional credits, meet all programme requirements, and demonstrate achievement of the exit level outcomes before the qualification can be awarded.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Horizontal Articulation (Graduates of this qualification may articulate horizontally into related qualifications at the same level, subject to institutional admission requirements and credit transfer policies.)

- Bachelor of Science in Computer Science
- Bachelor of Science in Information Technology
- Bachelor of Science in Cyber Security
- Bachelor of Science in Data Science
- Bachelor of Science in Software Engineering
- Bachelor of Science in Information Systems
- Bachelor of Science in Computer Networks and Security
- Bachelor of Science in Risk Management
- Bachelor of Science in Digital Forensics
- Bachelor of Science in Information Security and Assurance

Vertical Articulation (qualifications to which the holder may progress to)

- Master of Science International Risk and Security Management
- Master of Science (Hons) Cyber Security and Forensic Computing
- Master of Science in Risk, Crisis and Resilience Management
- Master of Science in Crisis and Disaster Management
- Doctoral studies (NCQF Level 9) in Information Security, Technology Policy, or ICT Management (for Level 8 graduates).

Holders of this qualification can pursue employment in various sectors including government, finance, telecommunications, education, health, and private enterprises, in roles such as:

1. Cybersecurity Analyst / Technician
2. Network Security Administrator
3. Information Security Officer

4. Systems Auditor / Compliance Officer
5. Risk Management Officer
6. Cyber Forensics Investigator
7. IT Infrastructure or Cloud Security Specialist
8. Penetration Tester / Ethical Hacker
9. ICT Security Consultant or Advisor
10. Security Policy and Governance Specialist

At advanced levels (NCQF Level 8 and above), graduates may assume supervisory, managerial, or research roles, such as:

- Cybersecurity Project Manager
- Chief Information Security Officer (CISO)
- Security Risk and Compliance Manager
- ICT Security Researcher / Lecturer / Trainer

Lifelong Learning and Professional Development

The qualification encourages continuous professional growth through engagement with industry certifications such as:

- CompTIA Security+, Network+, CySA+
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Certified Information Security Manager (CISM)
- Cisco Certified Network Associate (CCNA Security)

These certifications complement formal academic progression and enhance employability in the dynamic field of cybersecurity and ICT risk management.

QUALIFICATION AWARD AND CERTIFICATION

Qualification Award

To be awarded the Bachelor of Science in Cyber Security and Risk Management, a candidate must successfully attain a minimum of 505 credits and meet all qualification requirements.

Certification

The institution commits to issuing a certificate to candidates upon successful completion of the qualification.

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

Summary of Local, Regional and International Comparability

The proposed Bachelor of Science in Cyber Security and Risk Management at New Era College is comparable to both the Bachelor of Science in Cybersecurity and Risk Management – University of South Africa and the Bachelor of Science (Hons) Cyber Security and Forensic Computing –

University of Portsmouth. The qualifications share common areas such as cyber security, networking, digital forensics, ethical hacking, risk management, governance, and professional practice. However, the New Era College qualification is distinguished by its higher credit value, stronger focus on risk management and governance, and the inclusion of compulsory Industrial-Based Learning, which enhances practical exposure and graduate employability.

1. **Regional Qualification**

The Bachelor of Science in Computing offered by the University of South Africa is a **360-credit NQF Level 7 qualification, normally comparable to a three-year undergraduate degree, with a maximum completion period of eight years.** It is therefore comparable to the proposed New Era College qualification in terms of level, undergraduate degree status, and computing-related academic orientation.

The UNISA programme provides learners with a foundation in computing, computer science, information systems, programming, computer systems, and related technical areas. It is relevant for comparison because cyber security and risk management require strong computing knowledge, including programming, systems thinking, networks, information systems, and problem-solving. The proposed New Era College qualification builds on similar computing foundations but is more specialised because it focuses directly on cyber security, risk management, digital forensics, governance, cyber law, and Industrial-Based Learning.

In terms of credits, the UNISA qualification carries **360 credits**, while the proposed New Era College qualification carries **505 credits** for this submission. The higher credit value of the proposed qualification is justified by its broader scope and inclusion of a compulsory Industrial-Based Learning component. The New Era College qualification is also positioned at **NCQF Level 7**, which makes it comparable to the UNISA qualification at **NQF Level 7**.

2. **International Qualification**

The Bachelor of Science (Hons) Cyber Security and Forensic Computing offered by the University of Portsmouth is a **3-year full-time undergraduate honours degree, or 4 years with a sandwich/placement route. It carries the standard UK honours degree credit value of 360 credits**.

The University of Portsmouth programme is comparable because it prepares graduates with technical and investigative skills in cyber security, ethical hacking, digital forensics, forensic computing, networking, and cybercrime investigation. The programme includes modules such as **Computer Systems – 30 credits** and **Computing Foundations with Cyber Security – 30 credits**, showing that it uses credit-bearing modules within a structured undergraduate degree.

The programme is similar to the proposed New Era College qualification in areas such as cyber security, networking, digital forensics, ethical hacking, practical computing skills, project work, and professional practice. However, the University of Portsmouth qualification is more technically focused on cyber security and forensic computing, while the New Era College qualification has a broader focus by combining cyber security with risk management, governance, legal and ethical issues, entrepreneurship, research, and Industrial-Based Learning.

Assessment in the University of Portsmouth qualification includes coursework, practical assessments, laboratory work, projects, presentations, and examinations. Students are required to pass the prescribed modules and meet the university's progression and award requirements. Graduates may progress to postgraduate studies in cyber security, digital forensics, forensic computing, computer science, or related fields, and may seek employment as cyber security

analysts, digital forensic analysts, ethical hacking specialists, network security officers, and cybercrime investigation support officers.

3. **Proposed Qualification**

The proposed qualification is the **Bachelor of Science in Cyber Security and Risk Management** – New Era College of Arts, Science and Technology. It is positioned at NCQF **Level 7** and carries a total of **505 credits**, including a compulsory Industrial-Based Learning component. The purpose of the qualification is to produce graduates with advanced knowledge, skills, and competence in cyber security, risk management, cybercrime prevention, digital forensics, governance, research, and professional practice.

The programme covers areas such as cyber security, risk management, computer systems, networking, programming, digital forensics, ethical hacking, cryptography, governance, cyber law, entrepreneurship, research, and Industrial-Based Learning. It includes fundamental computing and programming modules, core cyber security and risk management modules, research components, practical modules, and workplace-based learning.

Assessment will be conducted through continuous assessment, practical work, assignments, tests, projects, examinations, research work, and workplace-based assessment during Industrial-Based Learning. To be awarded the qualification, candidates must attain a minimum of 505 credits and meet all qualification requirements. Graduates may progress to postgraduate diplomas or master's degrees in cyber security, information security, digital forensics, computer science, information technology, risk management, or information technology management. They may also be employed as cyber security analysts, risk officers, information security officers, digital forensic assistants, network security officers, compliance officers, IT auditors, security administrators, or cybercrime investigation support officers.

Overall Comparability Statement

The proposed Bachelor of Science in Cyber Security and Risk Management at New Era College is comparable to both the regional and international qualifications reviewed. All three qualifications share common areas such as cyber security, networking, digital forensics, ethical hacking, risk management, governance, professional practice, and graduate employability. However, the New Era College qualification is distinguished by its higher credit value, broader emphasis on risk management and governance, entrepreneurship components, and compulsory Industrial-Based Learning. These features make the qualification locally relevant, regionally responsive, and internationally aligned.

REVIEW PERIOD

This qualification shall be subject to periodic review to ensure that its content, structure, and learning outcomes remain relevant to industry needs, technological developments, and national policy priorities.

- The review period for this qualification is every five (5) years from the date of registration or re-accreditation with the Botswana Qualifications Authority (BQA).
- The review will be conducted by the Education and Training Provider (ETP) in consultation with relevant stakeholders, including industry representatives, academic experts, professional bodies, and regulatory authorities.

- Interim reviews may be carried out earlier if significant changes occur in:
  - National or international cybersecurity standards and frameworks;
  - Technological advancements within the ICT and cybersecurity sectors;
  - Labour market demands or skills gap analyses;
  - BQA policies, NCQF level descriptors, or assessment guidelines.
- Findings from the review process will inform updates to curriculum design, assessment strategies, learning outcomes, and credit allocation, ensuring continued alignment with NCQF requirements and global best practices.

(Note: Please use Arial 11 font for completing the template)

For Official Use Only:

CODE (ID)			
REGISTRATION STATUS	**BQA DECISION NO.**	**REGISTRATION START DATE**	**REGISTRATION END DATE**
LAST DATE FOR ENROLMENT		**LAST DATE FOR ACHIEVEMENT**	