SECTION A:	***QUALIFICATION DETAILS***																	
QUALIFICATION DEVELOPER (S)	NEW ERA COLLEGE																	
TITLE	Bachelor of Science in Cyber Security and Risk Management															***NCQF LEVEL***	*7*	
FIELD	Information and Communication Technology		***SUB-FIELD***	Cyber Security												***CREDIT VALUE***	*484*	
New Qualification			√	*Review of Existing Qualification*														
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

RATIONALE:

The Botswana Government has given serious attention on how to deal with the challenges of crime reduction in its National Development Plan II of 2017 – 2023. People with the skills of dealing with challenges of cyber-crimes are scarce in Botswana hence the need for the introduction of a cyber security and risk management degree. This qualification is to prepare students for a career in dealing with cybercrimes and risk management issues in both private and public institutions. Graduates will be able to apply knowledge gained in this programme to eliminate cybercrimes confronting most organisations. In the same vein, they will be able to guide organisations on how to eliminate the various risks that could obstruct organisations from achieving their goals and objectives.

An integrated crime control strategy that entailed crime prevention and detection, law enforcement and related collaboration with other partners was implemented during NDP 10. Specific crime reduction strategies included: Strengthening of law enforcement agencies, robust communication for effective information dissemination, strategic partnerships, and taking advantage of advances in technology to improve service delivery procedures. Progress made under the implementation of strategies adopted for NDP 10 included the following:

- In order to strengthen law enforcement agencies to deal effectively with crime through a rigorous proactive strategy, a number of units were established to deal with emerging crimes including cybercrime.
- The automation of identification of fingerprints was concluded in 2019, and this has improved turnaround times of processing of security clearance and criminal identification.
- A safer city programme is being rolled out for use in crime prune public places.
- In order to enhance the effectiveness of law enforcement, a number of laws were enacted. These included: Proceeds and Instruments of Crime Act No 28 of 2014, Forensic Procedures Act No. 31 of 2014 and Private Security Service Act of 2015.
- The efforts made to mobilise communities and the general public of Botswana to promote support for beneficial consultation and cooperation have resulted in an increase in the level of community involvement in the fight against crime.

To successfully achieve the above challenges, Botswana Government needs specialist in cyber security; safety and risk management who have the skills to conduct research in those areas and advice both the government and other organisations in Botswana, the SADC region, and African continent and beyond.
This is one of the objectives that our degree programme in cyber security, safety and risk management intend to achieve.

UNITED NATIONS
The qualification also aims to support the capacity building, awareness and implementation of the international multi bilateral environmental agreements that Botswana is a signatory to, which include but are not limited to:

- AUCAL – African Union Convention on Prevention and Combating Corruption
- UNODC – United Nations Office on Drugs and Corruption
- UNCAC – United Nations Convention Against Corruption
- CAACC – Commonwealth Africa Anti-Corruption Centre

The National Strategic Vision 2016 and Particularly Long Term Vision 2036

PILLAR 4 – GOVERNANCE, PEACE AND SECURITY

The Cybercrime and Computer Related Crime Act 2018 support the Government of Botswana drive to eliminate all forms of cybercrime and computer related offence. It is considered a serious offence for anyone to be involved directly or indirectly with cybercrime.

Apart from the cybercrime and Computer Related Crime Act, 2018, the NDP II and Vision 2036 also indicate its plan in combating cybercrime. The above NDP II shows clearly that cybercrime is a global growing threat as

experienced with computer viruses such as Melisa and Chernobyl, which have attacked isolated and networked information system through the internet or through software carriers and devices. Many vital decision-making processes of Government are now ICT based, and therefore vulnerable to this threat.
The government of Botswana plans to have the manpower to implement and monitor the activities surrounding cyber security, and risk management in both the public and private sector.

The individuals needed to implement the cybercrime and Computer Related Act 2018 must have a good academic background in the field of cyber security and risk management. People with these skills are scarce in Botswana and it is because of the scarcity of these skills that we have decided to develop a degree programme that will produce the necessary skills to meet the challenges Botswana is currently facing in the field of cyber security, safety and risk management.
Apart from students from Botswana, this degree will also attract students from other SADC countries and beyond. The programme will attract large number of potential candidates since there is little or no competition with other institutions in the SADC region.

PURPOSE:

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

- Apply critical thinking and logic to analyse and solve cyber security and risk management problems in both financial and non-financial security sectors
- Be globally competitive and employable in the labour market
- solve problems in cyber security, and risk management, locally and internationally.
- Utilise international best practices in cyber security, and risk management to combat crimes.

ENTRY REQUIREMENTS (including access and inclusion)

Full time Entry Requirements:

a) Certificate IV (NCQF level 4) with 6 subjects and passes in English, Mathematics and a Science subject or equivalent.
b) Applicants who do not meet the above criteria but possess relevant industry experience may be considered through Recognition of Prior Learning (RPL) and Credit Accumulation and Transfer (CAT) policies for access. This consideration will be done following guidelines of the ETP which are aligned with BQA/ National policies.

Recognition of Prior Learning (RPL) and CATS will also be provided for, and candidates will have to meet the necessary criteria set by individual ETPs in accordance with the BQA respective policies and regulations for RPL and CATS.

SECTION B	***QUALIFICATION SPECIFICATION***
GRADUATE PROFILE (LEARNING OUTCOMES)	***ASSESSMENT CRITERIA***
1. Analyse and solve cyber security and risk management problems in both financial and non-financial security sectors	1.1 Implement the concepts of cyber security, safety and risk management at the workplace. 1.2 Execute the integrated crime control strategies to protect against cybercrime. 1.3 Carry out risk assessment process and safety measures in the workplace.
2. Utilize international best practice in cyber security and computer networking to resolve security issues.	2.1 Evaluate and monitor internal systems networks to optimize performance and network compliance. 2.2 Identify the appropriate physical security controls to protect assets and facilities of the organization from threats 2.3 Recover critical systems to ensure business continuity from threatsand unpredictable incidents 2.4 Critique the usage of monitoring software to enforce proper behaviour in the workplace
3. Develop policies and procedures to manage enterprise security risks.	3.1 Develop policies and strategies in line with cyber security standards and risk management.

	2 Identify existing standards bodies that regulate cyber security frameworks 3.3 Conform with established standards and best practices for increasing protection baseline in cyber security and risk management
4. Evaluate and develop security systems with an emphasis on ethics, social engineering vulnerabilities and training	4.1 Develop an ethical code of conduct to Identify ethical and unethical behaviour in cyber security 4.2 Evaluate the use of ethical guidelines to control professional behaviour in the workplace 4.3 Recommend improvements to protect individual rights to privacy and intellectual property
5. Evaluate and implement cyber security, safety and risk management procedures in organizations to protect assets	5.1 Assess the effects of cybercrime on the development of your community or workplace environment. 5.2 Evaluate the relationship between technology and cyber security in combating cyber-attacks. 5.3 Evaluate the effects of cyber security and asset protection in terms of intellectual property 5.4 Implement the information security skills (digital threat management, malware detection and prevention, communication, etc.) in dealing with cybercrimes in your community and workplace environment to enhance adherence to safety. 5.5 Draft a risk management register for organisations to fight cybercrime.
6. Apply cyber security and risk management techniques to enhance organizational security	6.1 Employ transactions log systems to monitor users within the organization.

	6.2 Critique opportunities and threats revolving around valuable information and related assets to minimize threats to safety. 6.3 Adopt and customize national security policies that provide direction in the enhancement of organizational security.
7. Design, develop, test and evaluate secure software systems.	7.1 Develop software's that handle threats within the organization. 7.2 Design databases that are secure and that support multiple users within organization 7.3 Perform a vulnerability analysis using networked operating of an organization to reduce breach in an organizational IT systems
8. Design, review, and implement structures and processes that can be adopted in preventing cybercrime in organizations	8.1 assess the workplace environment and Identify the nature of cybercrimes and how best to prevent it in your organization. 8.2 Indicate clearly the structures and processes to be adopted in preventing cybercrime in your community or workplace environment 8.3 Develop an integrated cybercrime control strategy from identified structures and control processes to fight cybercrime in the workplace environment. 8.4 Implement, monitor and review the integrated cybercrime control strategy in the workplace.

SECTION C	***QUALIFICATION STRUCTURE***					
COMPONENT	***TITLE***	***Credits Per Relevant NCQF Level***				***Total*** ***(Per** Subject/ Course/ Module/ Units)*
		Level [5]	***Level [6]***	***Level [7]***	***Level [8]***	
FUNDAMENTAL COMPONENT *Subjects/ Courses/ Modules/Units*	Communication and Technical Writing	10				10
	Basics for Corporate Security and Risk Management		10			10
	Introduction to computer in Cyber Security	10				10
	Cybercrime and Society	10				10
	Fundamentals of Information System security	10				10
	Computer Organization		10			10
	Technology and Cyber Security		10			10
	Operating Systems Concepts	10				10
	Business Mathematics		10			10
CORE COMPONENT	Computer Networks		10			10
	Programming languages for cyber security		10			10

Subjects/Courses/ Modules/Units	Introduction to Risk Analysis and Loss Prevention		10			10
	Security Policies and Implementation Issues		10			10
	Network security, firewalls and VPNs		10			10
	Information Systems and Strategy		10			10
	Security strategies in windows and Linux platforms			10		10
	Database fundamentals			10		10
	Principles of Security Management			10		10
	Auditing IT Infrastructures for Compliance			10		10
	Managing risk in information systems			10		10
	Internet Security			10		10
	Information and Knowledge Management			10		10
	Project Management			10		10
	Wireless and mobile device security			10		10
	Cyber Security and Workplace Safety programs			10		10
	Cyber security risk management			10		10

	Cyber Security and Asset Protection			10		10
	Legal issues in Cyber Security			10		10
	Cybersecurity Metrics and Evaluation			10		10
	Research Methods			10		10
	Ethical Hacking			10		10
	Crime Protection			10		10
	Incident Response and Investigation			10		10
	Workplace Safety Programs in Botswana and the SADC Region			10		10
	Institutional Security Management			10		10
	Research Capstone Project			16		16
	Industrial Attachment			40		40
	Dissertation			16		16
	Crisis and Emergency Management			10		10
	Entrepreneurship			10		10
	Innovation Management			10		10
	Advanced Risk Analysis and Loss Prevention			10		10

ELECTIVE/ OPTIONAL COMPONENT *Subjects/Courses/ Modules/Units*	Organizational Behavior			10		10
	Strategic Management			10		10
	Public Relations and Customer Care			10		10
	Criminology and Criminal Justice				12	12
	Forensic Accounting				12	12
	Fraud Investigation and Management				12	12

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	***Credit Value***
Level 5	50
Level 6	100
Level 7	322
Level 8	12
TOTAL CREDITS	***484***

Rules of Combination:

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

- Fundamentals modules have a total of = **90** Credits
- Core modules have a total of = **372** Credits
- Electives (Choose 2 Modules)

  have a total of = **22** Credits

Total number of credits = **484** Credits.

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

Assessment and moderation shall be carried as per ETP's policies, which are aligned to BQA/ National policies. The ETP will engage only BQA accredited assessors and moderators to carry out assessment and moderation.'

RECOGNITION OF PRIOR LEARNING

Candidates can gain part or whole qualification through the application of ETP's Recognition of Prior Learning (RPL) and Credit Accumulation and Transfer CAT policies which is in line with National Policies.

CREDIT ACCUMULATION AND TRANSFER

Credit Accumulation and Transfer CAT policy will be applicable

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Horizontal Articulation (related qualifications of similar level that graduates may consider)

- Bachelor of Science in Software Development with Cyber Security
- Bachelor of Arts in Safety, Security and Risk Management
- Bachelor of Science in Risk and Security Management

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

Employment Pathways

- Security architect.
- Penetration tester (or ethical hacker)
- Cryptography.
- Chief Information Security Officer.
- Security engineer.
- Security auditor (or forensic expert)
- Incident responder.
- Vulnerability assessor

QUALIFICATION AWARD AND CERTIFICATION

To be awarded a **Bachelor of Science in Cyber Security and Risk management**, a candidate must attain 366 credits to graduate. The following c**onditions of attaining credits for graduation should be fulfilled.**

Certification

A certificate will be issued to candidates upon successful completion of all requirements.

REGIONAL AND INTERNATIONAL COMPARABILITY

SUMMARY OF SIMILARITIES AND DIFFERENCES OBSERVED

1. University of Maryland Global Campus (US)- Bachelor of Science in Cybersecurity Management and Policy programme aims to equip the learner with the skills to manage people and technologies required to protect information, information systems, and infrastructures including the nation's critical cyber infrastructures. It is ideal for students who want to leverage previous work experience to move into a team leader, supervisor, or management position within a corporate organization or government agency. The General Education, core and elective modules are assessed by more than one component; these components include examination, portfolio assessment held at the end of each semester and the class test followed by assignments given to the learners. Prescribed hours for instruction and assessment of the students in all the modules must be completed for award of the qualification.

2. University of Portsmonth (UK) - BSc (Hons) in Risk and Security Management, the main learning exit outcomes are focussed mainly on cyber security, risk management and operational management. Fundamental components include strategic and operational management, cyber security investigations and counter fraud. All the first-year core modules must be passed before the learner can proceed to the second year. Assessment methods include written examinations at the end of each semester, assignments and class tests which is usually mid-semester test.

3. Laurea University (Finland) - Bachelor of Business Management in Safety, Security and Risk Management degree includes safety, security, and risk management core competence. To be able to work as a safety, security and risk management specialist, the university is of the view that the students must learn and understand the basics of business, entrepreneurship, customer driven service development, leadership, and the economy and business law. However, in the main studies students specialise in the content of safety, security, and risk management. The core modules include Basic of Corporate Security and Risk Management, Information and Cyber Security, Digital Services, Business and Marketing Strategy, Management and Leadership. The assessment methods include written examination at the end of each semester, class test and take-home assignments. At the end of the programme's students are expected to pass all the core modules which are compulsory before they can graduate.

Generally, the three programmes studied are similar in that they all cover the core modules that are fundamental to the degree programme. In addition to this, the programme uses examinations, assignment, and class test to assess the students.

The differences observed is the fact that in Laurea University in Finland, the degree programmes take $3^1/_2$ years whereas in Indiana University of Maryland Global Campus it is 5 years while in University of Portsmouth in U.K. it is $4^1/_2$ years. In Laurea University, students are given two opportunities before they complete the degree programme to participate in many different projects and development assignments with external partners and companies whereas in University of Maryland Global Campus and University of Portsmouth such opportunity does not exist.

COMPARABILITY AND ARTICULATION OF THE PROPOSED QUALIFICATION WITH THE ONES EXAMINED

The proposed qualification generally compares well with the three programmes or qualifications studied in terms of content scope to be achieved before assessment. The only difference between the proposed qualification and the ones studied is that it is drafted and tailored in such a way that it reflects the local need and experience of the Botswana manpower development and the needs of the local organizations. The proposed programme is 80% comparable with the three international universities highlighted about. The 20% difference being that New Era College programmes address local issues and problems facing security and risk management issues of the local industry needs in both the public and private sector of the economy. This program is designed to prepare the learner for vendor certification exams which are Internationally recognized, as these skills are on demand in global market helping them employable.

Finally, this proposed qualification offers a wide range of alternatives in which the students can specialize in their final year. To add on some modules in the programme are vendor certification based like Certified Network Defender, Certified Ethical Hacker, CHFI, CTIA, CSA as these skill are in demand thus increasing employable.

REVIEW PERIOD

The qualification will be reviewed after 5 years