BQA NCQF QUALIFICATION TEMPLATE

SECTION A:	QUALIFICATION DETAILS				
QUALIFICATION DEVELOPER (S)	Botswana Accountancy College				
TITLE	Bachelor of Science in Cyber Security and Digital Forensics			**NCQF LEVEL**	7
STRANDS (where applicable)	N/A				
FIELD	Information and Communication Technology	**SUB-FIELD**	Information Technology	**CREDIT VALUE**	480

New Qualification	✓	*Legacy 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:

Cybercrime is on the increase and set to keep growing as technology becomes more widespread. High-level security breaches targeting government entities, public services and corporations have occurred and are still occurring. Globally, cyber-crime is growing exponentially and according to Forbes magazine in 2023, the global cost of cybercrime is predicted to hit USD $8 trillion in 2023 and will grow to USD$10.5 trillion by 2025 [1]. At the national level, as contained in HRDC report of 2023, www.hrdc.org.bw , the HRDC identifed cyber cyber security as a critical skill that the industry needs now and in the future [2].

The African Cyber Security Institute also did a survey on the Information Technology, IT skills and the results pointed out that there is a is huge gap in cybersecurity skills around the country [3]. This is also corroborated by findings from the research done by KPMG African Cyber Security Outlook that showed

that many organisations in Africa have experienced some cyber-attacks these recent years [4]. The Cyber Security and Digital Forensics programme aligns well with Botswana's Vision 2036 and NDP11, emphasising on the transformation of the country from a resource-based economy into a knowledge-based economy (HRDC, 2023). With digital transformation, hackers attempt to break into the systems to compromise data and hence cyber security experts are needed to assist in making sure that IT systems are safe.

References

[1]. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=3248e1cf19db
[2]. The Future of Jobs Report, HRDC Report, 2024
[3]. https://thepatriot.co.bw/botswana-has-huge-cyber-security-skills-gap/
[4]. KPMG Africa Cyber Security Outlook Report, September 2022

PURPOSE: (itemise exit level outcomes)

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

1. Apply risk assessment methodologies and tools to select and configure security controls that safeguard an organisation's information assets.
2. Analyse and monitor an organisation's computer systems and network infrastructure for signs of cyber-attacks.
3. Conduct research on cyber security and digital forensics landscape to gain insights and knowledge of latest trends in the field.
4. **Create,** compile, and present digital forensics evidence acquired from digital assets of an organisation in a professional manner.
5. Apply knowledge of digital forensics investigation by responding to cyber security incidents and hence assist organis ations to trace digital footprints of perpetrators.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

Applicants should have **any one** of the following:

(a) Minimum entry level is NCQF Level 4 or equivalent.

OR

(b) Entry through Recognition of Prior Learning (RPL) and Credit Accumulation and Transfer (CAT) will be accessible to all learners through institutional policies in line with the national RPL and CAT policies.

SECTION B	***QUALIFICATION SPECIFICATION***
GRADUATE PROFILE (LEARNING OUTCOMES)	***ASSESSMENT CRITERIA***
1. Evaluate and conduct research in cybersecurity and digital forensics to gain insights and knowledge on latest trends in the field.	1.1 Conduct research to explore current and emerging trends in cybersecurity and digital forensics. 1.2 Analyse research findings and apply them to practical cybersecurity problems. 1.3 Develop a comprehensive research proposal, including problem identification, literature review, and methodology. 1.4 Present research findings clearly and concisely to a range of audiences.
2. Employ cyber security risk assessments methodologies and tools in accordance with international professional standards to mitigate cyber security risks in an organisation.	2.1 Utilise risk management standards and methodologies when conducting a cyber security assessment. 2.2 Perform penetration tests using the right tools to identify vulnerabilities and provide recommendations.

	2.3 Identify, analyze, categorize, and classify cyber security threats. 2.4 Develop a threat landscape for an organisation and account for its dynamic nature.
3. Communicate effectively in cybersecurity and digital forensics fora to simplify technical information to diverse stakeholders.	3.1 Participate actively in collaborative team activities and discussions. 3.2 Communicate technical information clearly to both technical and non-technical stakeholders. 3.3 Provide constructive feedback and support to team members to achieve collective goals. 3.4 Resolve conflicts and demonstrate leadership in managing team dynamics.
4. Create cybersecurity solutions within an organisation in compliance with international standards to address cyber security and digital forensics problems.	4.1 Develop security controls to safeguard systems and information. 4.2 Implement standards to strengthen security controls throughout the development process. 4.3 Identify common trade-offs and compromises when integrating security into existing systems. 4.4 Plan, manage and prepare for an incident response.
5. Analyse and interpret digital evidence and present findings in compliance with legal	5.1 Collect and preserve digital evidence following legal and ethical guidelines.

and ethical standards to resolve cyber security incidents in organisations.	5.2 Use forensic tools and techniques to analyse digital data from various sources. 5.3 Develop a structured approach to digital investigations, ensuring accuracy and integrity of findings. 5.4 Conduct a comprehensive forensic investigations report. 5.5 Prepare and present digital forensic reports suitable for legal proceedings
6. Evaluate and formulate cybersecurity policies and procedures to enhance and maintain an organisation's security posture.	6.1 Develop cybersecurity policies and procedures aligned with organisational goals and regulatory requirements. 6.2 Assess the effectiveness of existing cybersecurity policies and suggest necessary updates. 6.3 Train employees on cybersecurity policies, procedures, and best practices. 6.4 Monitor compliance with cybersecurity policies and handle policy breaches effectively.
7. Apply ethical and legal principles **in** all aspects of cybersecurity and digital forensics in compliance with regulatory requirements.	7.1 Identify and adhere to ethical standards and legal requirements in cybersecurity practices. 7.2 Evaluate ethical implications of cybersecurity decisions and actions. 7.3 Conduct digital forensic investigations in compliance with relevant laws and regulations. 7.4 Promote a culture of ethical awareness and responsibility within an organisation.

8. Use emerging technologies and innovative techniques to solve complex cybersecurity challenges in an organisation's network infrastructure.	8.1 Examine emerging threats and technologies in the cybersecurity landscape. 8.2 Use machine learning, artificial intelligence, and other advanced technologies to detect and mitigate cyber threats. 8.3 Integrate new cybersecurity tools and techniques to enhance existing security infrastructure. 8.4 Develop innovative solutions to address complex cybersecurity challenges.
9. Create a robust cybersecurity solutions in accordance with international standards **to** protect network infrastructure within an organization.	9.1 Develop and configure security controls to protect systems and information. 9.2 Use international security standards and best practices in the implementation of cybersecurity measures. 9.3 Identify and address vulnerabilities through continuous monitoring and updates. 9.4 Evaluate the effectiveness of implemented security solutions and recommend improvements.

SECTION C	QUALIFICATION STRUCTURE				
COMPONENT	TITLE	Credits Per Relevant NCQF Level			Total Credits
		Level [5]	Level [6]	Level [7]	
FUNDAMENTAL COMPONENT *Subjects/ Courses/ Modules/Units*	Introduction to Computer Technology	15			**15**
	Computer Related Mathematics and Statistics	15			**15**
	Systems Development	15			**15**
	Web and Multimedia Development	15			**15**
	Principles of Digital Forensics	15			**15**
	Fundamentals of Networking	15			**15**
	Professional and Ethical Issues in Computing	15			**15**
	Entrepreneurship and Business Accounting	15			**15**
CORE COMPONENT *Subjects/Courses/ Modules/Units*	Discrete Mathematics		*15*		**15**
	Linux Administration		*15*		**15**

	Mobile Forensics		*15*		***15***
	Introduction to Programming using Python		*15*		***15***
	Database Design and Development		*15*		***15***
	Ethical Hacking Essentials		*15*		***15***
	Secure Systems		*15*		***15***
	Research and Innovation		*15*		***15***
	Computer Systems Administration			*15*	***15***
	Artificial Intelligence for Cybersecurity and Digital Forensics			*15*	***15***
	Emerging Technologies			*15*	***15***
	Network Systems Administration			*15*	***15***
	Information Systems Auditing			*15*	***15***
	Research Project			*15*	***15***
	Industry Attachment			*60*	***60***
	Digital Forensics and Investigation			*15*	***15***
	Network and Cloud Forensics			*15*	***15***
	Cyber Threats Landscape			*15*	***15***

	Web Application Security			*15*	***15***
	Penetration Testing and Ethical Hacking			*15*	***15***
	Advanced Cybersecurity			*15*	***15***
STRANDS/ SPECIALIZATION	*Subjects/ Courses/ Modules/Units*	***Credits Per Relevant NCQF Level***			***Total Credits***
		Level [ ]	***Level [ ]***	***Level [ ]***	
1.					
2.					
Electives					

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	***Credit Value***
5	120
6	120
7	240
TOTAL CREDITS	480
Rules of Combination: ***(Please Indicate combinations for the different constituent components of the qualification)***	
Fundamentals - 120 credits. Core component - 360 credits. There are no modules under the elective component.	

ASSESSMENT ARRANGEMENTS
Formative Formative assessment will account for 60% of the final grade. **Summative** Summative assessment will contribute 40% of the total mark.
MODERATION ARRANGEMENTS
Moderation is done on all assessments that earn a learner grade towards attainment of the qualification. There will be both internal and external moderation of assessments. Assessors and moderators must be registered by Botswana Qualifications Authority or any other relevant and recognised body.
RECOGNITION OF PRIOR LEARNING
Candidates may provide evidence of prior learning and current competence and/or participate in suitable forms of Recognition of Prior Learning (RPL) assessment to earn credits toward the qualification, in line with applicable ETP RPL policies and the relevant national policy and legislative framework.
CREDIT ACCUMULATION AND TRANSFER
There is a provision for Credit Accumulation and Transfer, CAT, in accordance with institutional and national policies on CAT.
PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)
LEARNING **Vertical pathways** Upon completion of the qualification, graduates can progress into Bachelor of Science(Honours) degree and Master of Science qualifications in the field of Computer Science and Information Technology or Information Science. **Horizontal** Bachelor of Science in Computer Science Bachelor of Science in Information Security

Bachelor of Science Software Engineering

Diagonal

Upon completion of the qualification graduates can progress into Postgraduate certificate/diploma or Masters qualifications of other information technology disciplines.

Employment pathways

Upon completion, graduates can attain jobs in various computing and computing related disciplines.

- Cybersecurity specialists
- Information systems auditors
- InformationTechnology Analysts.

QUALIFICATION AWARD AND CERTIFICATION

To be awarded Bachelor of Science in Cyber Security and Digital Forensics**,** the learner must have attained a minimum of 480 credits.

If the candidate has met the minimum requirements to be awarded the qualification, a certificate will be issued.

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

The qualifications proposed for comparison have been selected based on their regional and international relevance. These qualifications are from institutions in the SADC region and internationally recognized bodies. The comparison includes qualifications that align with the Cyber Security and Digital Forensics field at NCQF Level 7 (equivalent to a Bachelor's degree). The selected institutions are recognized for their strong alignment with the standards developed by regulatory bodies such as the National Institute of Standards and Technology (NIST) in the U.S., ENISA (European Union Agency for Cybersecurity), and frameworks like the **ISC)** ² for cybersecurity professionals.

The proposed qualification was compared with the following:

1. Bachelor of Science in Informatics and Computer Security offered by Strathmore University,Kenya.
2. Bachelor of Science in Computer Science and Information Systems offered by University of Capetown, South Africa.
3. Bachelor of Science in Cyber Security Technology, from the University of Maryland Global Campus (United States of Africa)
4. Bachelor of Science in Digital Forensics and Cybersecurity from Eastern Kentucky University, United States of America.

Similarities

1. Core Focus on Cybersecurity and Digital Forensics

    - Observed: All benchmarked qualifications cover key subject areas such as network security, digital forensics, risk management, and ethical hacking.
    - Proposed Qualification: Similarly, the proposed program includes these modules as core components, positioning itself within international subject content expectations.

2. Practical and Industry-Driven Learning Approach

    - Observed: Institutions such as EKU and UMGC emphasize hands-on, applied learning through projects, simulations, and real-world case studies.
    - Proposed Qualification: This is matched by the proposed qualification's inclusion of capstone projects, practical labs, and simulated forensic investigations, ensuring learners are prepared for real-world challenges.

3. Alignment with International Standards and Competency Frameworks

    - Observed: qualifications align with standards such as NIST Cybersecurity Workforce Framework, ENISA Cybersecurity Skills Framework, and Seoul Accord.
    - Proposed Qualification: The proposed qualification also draws reference from international benchmarks and regulatory bodies such as NIST, ENISA, and QAA Computing Benchmarks, ensuring its relevance and comparability.

4. Career Pathways in Cybersecurity and Forensics

    - Observed: Graduates from the benchmarked programs are equipped for careers in incident response, digital forensics, IT security consulting, and cyber law enforcement.
    - Proposed Qualification: This is reflected in the proposed program's exit profile, which outlines graduate roles in cybersecurity operations, forensic analysis, and governance, supporting direct comparability in employment readiness.

5. Capstone Projects and Final Year Research

    - **Observed:** qualifications like UCT and EKU include final year projects that simulate real-world cyber challenges.

    - **Proposed Qualification:** Similarly, the program includes a Final Year Project module focused on applied research or forensic simulation, ensuring depth in learning and alignment with international pedagogy.

Differences

1. Duration and Credit Structure

    - Observed: African universities like Strathmore and UCT follow **a** 480-credit, 4-year system**,** while UMGC and EKU follow the 120-credit US model**.**
    - Proposed Qualification: It adopts the 480-credit structure aligned with NCQF Level 7**,** with a 4 year duration, making it regionally comparable but requiring clear articulation mechanisms when benchmarking with US programs.

2. Assessment Approaches

    - Observed: UMGC uses online quizzes and capstone projects**;** EKU uses practical assessments and case files**;** UCT and Strathmore employ traditional coursework and final exams**.**
    - Proposed Qualification: Combines traditional academic assessments with practical and scenario-based tasks but can improve by integrating case-based or industry-linked assessments similar to UMGC's approach for enhanced global articulation.

3. Integration of Industry Certifications

    - Observed: UMGC and EKU embed certifications such as CEH, CompTIA Security+, CISSP into the program content.
    - Proposed Qualification: Include embedded certifications in upon completion of modules such as Ethical Hacking Essentials (EHE), Penetration Testing and Ethical Hacking (CEH) and encourages students to pursue them.

4. Specialization Areas

    - Observed: EKU leans toward law enforcement and digital crime investigation**;** UMGC emphasises corporate cybersecurity and auditing**.**
    - Proposed Qualification: **Offers a** balanced focus**, blending digital forensics, policy, and technical modules. However, it could carve a niche by tailoring**

certain electives to regional threats, compliance laws (e.g., Botswana's Data Protection Act), or cross-border cybercrime**.**

Conclusion

The proposed B.Sc in Cyber Security and Digital Forensics mirrors global best practices in content and design. It aligns with both regional structures (480 credits, NCQF Level 7) and international expectations in terms of core subjects and graduate outcomes. To strengthen global articulation, the qualification also includes the integration of industry certifications**.**

Comparability and articulation of the proposed qualification with the ones examined

The proposed BSc in Cyber Security and Digital Forensics demonstrates strong comparability and alignment with internationally recognised cybersecurity and digital forensics qualifications. Based on the benchmarking against Strathmore University (Kenya), University of Cape Town (South Africa), University of Maryland Global Campus (USA), and Eastern Kentucky University (USA), key areas of comparability and articulation have been identified.

Progression and Career Articulation

- The proposed qualification enables articulation into postgraduate studies, similar to benchmarked qualifications that allow graduates to pursue:
  - Master's in Cybersecurity, Digital Forensics, or Information Security.
  - Professional industry certifications (CISSP, CEH, CISM, etc.).

Employment Pathways:

- The proposed qualification aligns with career paths in incident response, penetration testing, forensic investigations, and cybersecurity governance.
- EKU aligns with law enforcement & forensic investigation, while UMGC aligns more with corporate cybersecurity, offering different specialization routes.

(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**	
REVISION DATE:		**NAME OF PROFESSIONAL BODIES/REGULATORY**	