SECTION A:	QUALIFICATION DETAILS				
QUALIFICATION DEVELOPER	Botswana International University of Science and Technology				
TITLE	Bachelor of Science (Honours) in Information Security Management			NCQF LEVEL	8
FIELD	Information and Communications Technology	SUB-FIELD	Information Security Management	CREDIT VALUE	120
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

Developing countries such as Botswana are also experiencing cyber threats and need experts in the field. There is a demand for experts in Botswana who specialize in information security. This statement is supported by the documented discussions with the members of the BIUST Computer Science and Information Systems Departmental Stakeholder Advisory Committee (DSAC) held on October 13, 2016 and March 3, 2017, and the HRDC document on priority skills and employment trends which shows that Information Security Analysts and Cyber Security experts are among the jobs that will be required in the near future. Information Security Management qualification contributes to the achievement of the goals stated in the National Information and Communications Technology (ICT) Policy (Maitlamo) which calls for the protection of personal privacy and security of information systems and networks, NDP 11 and ETSSP.

The need for Information Security Management is also reflected in the HRDC documentation of priority skills and employment trends document, under the ICT sector of Table 4, which outlines the technical and soft skills for the top occupations in demand for Botswana. The Information Security Management qualification will produce highly skilled graduates who are capable of defending our critical information

technology infrastructure and this contributes to the National Vision 2036 Pillar 4. Criminal activities are getting complex with the advancement of technology hence the need for experts in the field of Information Security Management to be able to manage the defense and investigate crimes committed within the digital domain and this qualification is in line with the National Vision 2036 Pillar 4. There is also a high demand of Information Security managers worldwide. This statement is supported by the National Institute of Standards and Technology (NIST) version 1.1 2018.

The introduction of this qualification will place Botswana at the forefront on dealing with cyber threats. With the growing numbers and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information as well as safeguard national security. The proposed qualification will advance student's skills and expertise to safeguard the nations against cyber-attacks.
This qualification will provide candidates with highly specialized theoretical knowledge while they gain analytical skills to excel in areas within the information security domain. This qualification will imbue candidates with expertise to manage and identify breaches, vulnerabilities and threats and build the digital investigation expert skills that will minimize their impact on organizations. Furthermore, this qualification offers skills to candidates. It also empowers candidates to become entrepreneurs.

PURPOSE:

The purpose of this qualification is to produce graduates with highly specialized knowledge, skills and competences to:

- Apply information security management systems to protect information assets of large organizations.
- Monitor network infrastructure for advanced cyber-attacks.
- Perform digital investigation of advanced cyber-attack.
- Conduct advanced digital data extraction and analysis.

ENTRY REQUIREMENTS (including access and inclusion)

Minimum entry qualification is Bachelor degree, NCQF Level 7.

Recognition of Prior Learning (RPL) and Credit Accumulation and Transfer (CAT) will also be considered to enhance inclusion and access.

SECTION B QUALIFICATION SPECIFICATION	
GRADUATE PROFILE (LEARNING OUTCOMES)	***ASSESSMENT CRITERIA***
1. Apply highly specialized practical, conceptual and technological understanding to create security roles, procedures and management structures appropriate in a medium to large organization.	1.1 Design strategic organizational planning for information security management and its relationship to organization-wide and IT strategic planning 1.2 Identify the organization's key stakeholders and their roles. 1.3 Develop a complete information security program for a medium to large organization, along with its importance, benefits and desired outcomes of the said security program to the organization. 1.4 Develop information security policies and their roles in a successful information security program. 1.5 Implement different types of security policies and the major components in each.
2. Operate in a complex environment and unpredictable contexts to select identification and authentication technologies appropriate for a medium to large organizations.	2.1 Apply CIA triage to each component of large-scale environment. 2.2 Apply the common properties used for authentication. 2.3 Implement both physical and logical access list in a medium to large organizations.
3. Provide original and creative critical responses to the task of developing an appropriate business continuity and disaster recovery plan for a medium to large organization.	3.1 Demonstrate the principal components of the Information security system implementation planning. 3.2 Implement business contingency planning methods in a medium to large business enterprises. 3.3 Design business contingency plans with the relevant stakeholders.

4. Undertake analysis of complex, incomplete and contradictory evidence/ data and argue for a scheme of risk management appropriate for a medium to large organization.	4.1 Develop risk management guidelines and how they are implemented in the organization. 4.2 Use risk management guidelines to implement the necessary techniques to identify and priorities risk factors for information assets and the assessment of those risks. 4.3 Apply popular methodologies used in the industry to manage risk.
5. Operate in a complex and unpredictable context to select physical and environmental security measures appropriate for a medium to large organization.	5.1 Relate the organization's hardware devices into physical components and how such components can be protected. 5.2 Determine the vulnerabilities associated with various physical components interfaces. 5.3 Incorporate various cyber security legislation 5.4 Design a structured approach to managing security risks and information technology operations within the context of an organization's objectives.
6. Contribute meaningfully when working as a member of a team.	6.1 Demonstrate tolerance to viewpoints expressed by other members of the team 6.2 Provide assistance and encourage other team members. 6.3 Contribute towards group deliverables. 6.4 Demonstrate leadership skills and ability to manage conflicts in group tasks.

SECTION C	QUALIFICATION STRUCTURE				
	TITLE	Credits Per Relevant NCQF Level			Total (Per Subject/ Course/ Module/ Units)
		Level [ ]	Level [ ]	Level [8]	
FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Not Applicable				
CORE COMPONENT Subjects/Courses/ Modules/Units	Individual Research Project in Information Security and Management			30	30
	Group Project in Information Security			24	24
	Risk Management			13	13
	Human and Organizational Aspects of Information Security			13	13
	Information Security I			13	13
ELECTIVE/ OPTIONAL COMPONENT Subjects/Courses/ Modules/Units	Internet of Things Security			9	9
	Malware Analysis			9	9
	Privacy in Digital Age			9	9
	Data Visualization Analytics			9	9
	Knowledge Security			9	9

	Practical Applications in Information Security Management			9	9
	Strategic Security and IT Management			9	9
	Compliance and Legal Issues			9	9

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	***Credit Value***
Core	***93***
Elective	***27***
TOTAL CREDITS	***120***
Rules of Combination: ***(Please Indicate combinations for the different constituent components of the qualification)***	
All core modules are from level 8 and are compulsory (93 Credits). Students choose 3 electives (27credits), also from level 8.	

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.

Formative Assessment

Formative assessment or continuous assessment contributing towards the award of credits should be based on course outcomes. This can include tests, assignments and projects as well as simulated and real work settings. The contribution of formative assessment to the final grade shall be 40%.

Summative Assessment

Candidates may undergo assessment including written and practical and simulated projects. The final examination contributes 60% of the final mark.

MODERATION ARRANGEMENTS

There shall be internal and external moderation as a quality assurance measure in accordance with relevant provider policies.

Assessors and moderators must be suitably qualified in the area of information security management.

RECOGNITION OF PRIOR LEARNING (if applicable)

Recognition of Prior Learning (RPL) and Credit Accumulation and Transfer (CAT) will be applicable for award of this qualification. Candidates may submit evidence of prior learning and current competence and/or undergo appropriate forms of RPL assessment for the award of credits towards the qualification in accordance with applicable provider RPL policies and relevant national-level policy and legislative framework. Implementation of RPL shall also be consistent with requirements, if any, prescribed for the field or sub-field of study by relevant national, regional or international professional bodies.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Learning Pathways

Horizontal Articulation: (NCQF Level 8).

- Bachelor of Science (Honours) in Cyber Security.
- Bachelor of Science (Honours) in Digital Forensics.

- Bachelor of Science (Honours) in Computer Science.

Vertical Articulation: (NCQF Level 9).

- Master of Science in Information Security Management.
- Master of Science in Cyber Security.
- Master of Science in Digital Forensics.
- Master of Science in Computer Science.

Employment Pathways

There are several opportunities in for the specialists in Cyber Security and Digital Forensics including:

- Information Security Analyst
- Information Security Engineer
- Penetration Tester
- Vulnerability Research Engineer
- Computer Systems Security Analyst
- Threat Intelligence Analyst
- Insider Threat Analyst
- Security Incident Responder
- Business Process and Security Analyst
- Risk Manager Analyst
- Security Operations (SOC) Analyst
- Healthcare Information Systems Security Officer
- Web Mobile Application Security Engineer
- Malware Analyst
- Disaster Recovery Analyst
- Digital Forensics Investigator
- Industrial Cyber Security Analyst
- Network Security Analyst
- Cyber Security Architect
- Cloud Security Engineer
- Exploit Engineer
- Secure Software Developer
- Cryptographer

- Entrepreneur

QUALIFICATION AWARD AND CERTIFICATION

Minimum Standards of Achievement for the Award of the Qualification

To be awarded a Bachelor of Science (Honours) Information Security Management degree, a candidate is required to achieve a minimum of **120** credits inclusive of 93 credits for Core courses, and 27 credits for Optional/ Elective Courses.

Certification

Candidates meeting prescribed requirements will be awarded the qualification in accordance with standards prescribed for the award of the qualification and applicable policies. Candidates who do not meet the prescribed minimum standards will be issued a transcript only.

REGIONAL AND INTERNATIONAL COMPARABILITY

Benchmarking

1. University of Maryland Global Campus, Bachelor of Science in Cyber Security Management and Policy.
2. Solent University (Southampton), Bachelor of Science (Honours) in Cyber Security Management.
3. University of Richmond, Bachelor of Science Professional Studies measuring in Information Security.

Regional

There is no university within the region that offers Bachelor of Science Honours in Information Security Management.

International

Majority of the top international universities do not offer Information Security Management as Bachelor of Science Honours, but rather they offer the qualification as either Bachelor of Science honours in Cybersecurity Management or just Bachelor of Science Information Security. The listed universities above are some of those benchmarked within the equivalent qualification.

University of Maryland Global Campus and Solent University are some of the top public universities which existed over 75 and 100 years respectively that offer Bachelor of Science Honours in Cybersecurity Management. Therefore, it is relevant to benchmark with these universities to identify the common features as well as need for improvement.

The core features and syllabi of the course is closely identical as indicated in the benchmarking table presented in following paragraphs and hence every module and content is matched to have an in-depth analysis on each and every topic associated with the innovations and learning new concepts of the course for the benefit of the students. Hence matching with one-to-one comparisons are carried out and the benchmarking table is presented.

Similarities with the proposed qualification

The major similarity between the proposed qualification and the qualifications benchmarked with is the list of modules offered. Most of the modules are similar despite the differences in the naming of those modules, and such modules are offered at advanced stages in all the qualifications

Differences with the proposed qualification

The proposed qualification is a progression from Bachelor of Science in Cyber Security and Digital Forensics. Therefore, entry to this qualification requires the learner to have at least 4 years of Bachelor of Science in Cybersecurity and Digital Forensics or equivalent. The proposed qualification is therefore a 1-year qualification whereas in other benchmarked qualifications the duration of the qualification is 3 years or 4 years with placement. With the proposed qualification, the foundation courses are covered in Bachelor of Science in Cyber Security and Digital Forensics and the advanced courses are left for the proposed qualification, while the benchmarked qualifications bundle both foundation and advanced modules in one qualification.

Conclusion:

After the benchmarks, it can be concluded that the proposed qualification is better structured since the learners will gain more knowledge on the foundations courses first before they move to the proposed qualification which is advanced. The number of both foundation and advanced modules are more on the proposed qualification than on the benchmarked qualifications, and they are stretched over a longer duration and thereby giving learners to the concepts better before they move to the next stage.

REVIEW PERIOD
5 years in line with the NCQF.