1 QUALIFICATION SPECIFICATION SECTION A							
QUALIFICATION DEVELOPER	Limkokwing University of Creative Technology						
TITLE	Bachelor of Science in Information Technology Security				**NCQF LEVEL**	7	
FIELD	Information and Communication Technology		**SUB-FIELD**		Information Technology Security		
New qualification	✓	Review of existing qualification					
SUB-FRAMEWORK	General Education		TVET		Higher Education	✓	
QUALIFICATION TYPE	Certificate		Diploma		Bachelor	✓	
	Bachelor Honours		Master		Doctor		
CREDIT VALUE					**500**		

RATIONALE AND PURPOSE OF THE QUALIFICATION

1.1 Rationale of the Qualification

Botswana has over the years seen increased uptake of information and communication technology (ICT) and its associated services. This has seen ICT become an integral part of daily lives, personal and corporate, used in various aspects such as communication, shopping, banking, data storage, marketing, and advertising to mention a few. The country has seen an increasing number of criminal acts performed using ICT, against both individuals and corporations. A 2018 report by Modley (a global leader in network and endpoint security) indicates that 63 percent of Botswana businesses were hit by cyber-attacks in 2018, classifying Botswana among African countries most hit by cyber-attacks in that year. A 2017 report by Checkpoint revealed Botswana accounted for 3 percent of all cyber-attacks on the African continent and ranked eighth among Africa's ten biggest sources of cyber-attacks (Sunday Standard, 25 March 2019). At a stakeholder's workshop held in January 2019 to discuss the National Cyber security Strategy, Botswana Police Services indicated that they have registered 143 reported cases between 2015 and 2018. Despite this there are "…less than 30 certified practicing digital forensic examiners in the country with almost 80 percent of them in law enforcement agencies including Botswana Police Service, Directorate on Corruption and Economic Crime, Directorate of Intelligence and Security and the Botswana Defence Force" (Botswana Guardian, 29 January 2019).

a) Human Resource Development Council Report on Need for Information Technology Security Skills

Botswana National Development plan 10 and 11 advocated for development of skills aligned to the country labour market based on the Human Resource Development Strategy survey administered by the Human Resources Development Council (HRDC, 2016). ICT security was amongst those areas identified as a key area for skills development. Naturally these would encompass ICT security Manager, Data Centre Manager and Computer Network Professionals as requisite occupational areas according to HRDC report on Top Occupations in Demand according to the ICT industry in Botswana, refer to figure 1 below.

b) National Cyber Security Strategic Report

The Ministry of Transport and Communication (MTC) as the custodian and implementer of National ICT implementation drive and utilization of ICT in Botswana held an ICT Pitso Forum to review progress on the national ICT enactment, developments, and ICT initiatives in the country from the 25th to 26th of August 2015. Information Technology security constitute cyber security was addressed as the country's challenged area. One of the conclusions drawn upon the presentations done was the country is still vulnerable to Cyber Security attacks because there is no adequate and technical skilled manpower to manage and thwart cyber security attacks according to the National Cyber Security Strategy Report. The end result or impact was minimum utilisation of ICTs at Government, Business, and Individual levels according to the World Economic Forum Reports (WEF, 2013 & 2014)

c) National Newspapers on Cyber Security

Both national newspapers of Botswana namely, The Sunday Standard, The Patriot and The Guardian have commented on the increase in issues related to cyber security. The Guardian in its editorial release of 29th August 2019 mentioned of a prevailing environment indicating that cybercrime is a real problem in Botswana with statistics indicating an increase in registered cases for the past four years - 56 registered cases by September 2018, 39 registered in 2017, 25 in 2016 and 23 in 2015. The Patriot of 11thSeptember 2019 reported titled "'Botswana has huge cyber security skills gap" a survey poll conducted showed that 40% of the organisations have never trained their ICT personnel on cyber security while 30 % resorted to training only when they face a problem. The Sunday Standard newspaper of 26thAugust 2019 reported that Botswana accounted for 3% of all cyber-attacks on the African continent. This development calls upon human capacity development in information Security that could be recruited by various organizations to manage and monitor Information Technology Security problems and protection in Botswana.

d) National Development Plan 10 and 11 (2010-2023)

National Development Plans (NDPs) are series of the nation strategic developments which highlight key strategic goals which should be implemented based on national needs and aspirations. The NDP10 strategic plan advocated adoption and fostering for ICT as a tool for Botswana's economic diversification from non-renewable-resource driven economy to a knowledge driven economy. This calls upon an implementation of Information Systems that provide a host of services to the nation as it drives towards a contextualised Botswana Information Society Community realised in the form of e-Government, e-Legislation, e-Education, e-Health, e-Commerce, e-Agriculture, and e-Tourism. According to NDP10 this can only be realised through human capital development of most critical ICT skills like "...ICT (software development, hardware development) by virtue of the complex information system architectures there is need for complex information security, information technology devices and communication channels security support through personnel like IT Network Administrator, forensic specialists (ICT), secure software developers, and Penetration and Vulnerability Tester.

e) Botswana National Information and Communication Technology Policy: Maitlamo Policy 2007

The National Information and Communication Technology (ICT) policy, (Maitlamo Policy, 2007) provides Botswana with a clear and compelling roadmap that drives the social, economic, cultural, and political transformation through planning and implementation of contextual and effective ICTs in terms of human resource development, infrastructural planning and utilisation. The National ICT Policy's Vision is: "Botswana will be a globally-competitive, knowledge and information society where lasting improvements in social, economic and cultural development are achieved through effective use of ICT". Implementation of the ICT initiatives has had the following effects to Botswana

- Increase in the number of organisational computer systems connected to the Internet with many unaware of security compliance standards, the convergence of image, voice and data communications systems and the reliance of organizations in Botswana on those systems
- Emerging threat of sophisticated adversaries and criminals seeking to compromise those systems
- The sharing of infrastructures, services, and information between government and industry

f) Consultations with Stake Holders

Institutional consultations with the ICT industry identified the hard and soft skills needed for information technology security in the industry. The industry needs graduates who have analytical network and data security skills, decoding and coding techniques, hacking skills, data management, web and mobile security implementation skills, software programming skills, verbal and written communication skills, analytical and problem-solving skills, managerial, project management and research-based skills, etc. Because information technology security evolves rapidly graduates need to be lifelong learners who can combine technical expertise with context-sensitive soft skills in order to cope with complex situations in real life.

This qualification is in line with local, regional, and international industry demand and will equip learners with deeper insight into the core areas of information technology security discipline. The qualifications shall also provide guidance in application of acquired research skills in information technology security, thus creating new knowledge in key and specific contexts. The ever-evolving information technology security threats have led to the need for developing skills and competency to thwart attacks on information security threats, information technology devices and communication channels. Many companies now recognise generally and professional information technology security skills as highly strategic and driver of any knowledge-based economy and information society.

1.2 Purpose of the qualification

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

a) Protect information systems developed, data communication networks, software applications and data storage provisions in order to ensure proper utilization and guarantee a smooth Botswana Knowledge based economy and Information Society transition in line with the aspirations of the National ICT Policy.
b) Execute tasks related to the application of IT security implementation through applying relevant techniques, theories, and methodologies.
c) Evaluate, identify, and manage IT security threats and provide solutions.
d) Apply innovation and creativity to develop unique IT security solutions to solve clients' problems.
e) Work as members of a project team and observe the ethical and professional codes of the IT security industry.

2 ENTRY REQUIREMENTS (including access and inclusion)

2.1 Entry Requirements:

- Normal Requirements Certificate IV (NCQF Level 4) or equivalent.

2.1.2 Recognition of Prior Learning (RPL)

Applicants who do not meet the above criterion but possess relevant industry experience may be considered using RPL and CATS policies for access. This will be done following consideration of the ETP, aligned with BQA policies.

3 QUALIFICATION SPECIFICATION SECTION B

GRADUATE PROFILE (LEARNING OUTCOMES)	ASSESSMENT CRITERIA
3.1 Protect organizational data at rest, during processing, and in transit	3.1.1 Implement cryptographic protocols, tools and techniques appropriate information security measures for a given organisational situation. 3.1.2 Configure end-to-end security protocols appropriate for a given organisational situation 3.1.3 Evaluate various computer forensic software tools and techniques as well as follow proper legal procedures for obtaining, analyzing, and reporting digital forensic evidence 3.1.4 Assess security controls for an information system to provide assurance where the security processes or controls are implemented 3.1.5 Apply appropriate technique for data erasure for a given organisational situation.
3.2 Develop software that reliably preserves the security properties of	3.2.1 Apply appropriate fundamental security design principle for a given software development scenario.

the information and systems it protects	3.2.2 Choose an appropriate security technique for including in the design of software for clients. 3.2.3 Select appropriate techniques for including security considerations throughout the implementation of software. 3.2.4 Test implemented software security measure for validating fulfillment of security requirements and specifications defined by the client. 3.2.5 Explore security issues in the use of software, and in its deployment, maintenance, and removal. 3.2.6 Present consequences of security-related choices based on ethical considerations in software security to stakeholders 3.2.7 Provide reasoned advice on alternatives of dealing with consequences of security-related choices based on ethical security considerations.
3.3 Design security models to implement and interface components integrated into larger existing systems.	3.3.1 Apply various activities in phases of a component's lifecycle when integrating systems. 3.3.2 Evaluate techniques for protecting the design elements of an integrated circuit. 3.3.3 Identify security risks in a component supply chain. 3.3.4 Apply optimum techniques for testing security properties of a component before and after integrating it into a system. 3.3.5 Reverse-engineer systems based on minimal outside information.
3.4 Evaluate the computer network and information security needs of an organization.	3.4.1 Compare the components and interfaces of the OSI and TCP/IP networking models. 3.4.2 Install computer network physical component and their associated vulnerabilities. 3.4.3 Apply principles of Internet 5-layer model, as software components and interfaces that represent levels of services encapsulated by lower-level services.

	3.4.4 Justify how a specified standard interface could expose vulnerabilities in a software component during interfacing of subsystems. 3.4.5 Detect data transmission attacks on components that provide the service of relaying information.
3.5 Ensure a system can function under disruptive conditions associated with misuse and malicious behavior	3.5.1 Detect vulnerabilities of functional system as a whole and subcomponents connected to it. 3.5.2 Evaluate the techniques for including security considerations throughout the maintenance and management of the system. 3.5.3 Identify entities, and confirm that identification to the desired level of granularity 3.5.4 Detect, compensate for, defend against, and prevent system attacks. 3.5.5 Evaluate the effects of retiring a system at or before its end of life on the security of other systems, or of the organization that used the system.
3.6 Protect individuals' data and privacy in the context of organizations (i.e., as employees) and personal life	3.6.1 Develop measures to counter system access attacks and mitigation measures. 3.6.2 Implement approaches for detection and mitigation of social engineering attacks. 3.6.3 Conduct cyber hygiene, Cyber Security user education, as well as cyber vulnerabilities and threats awareness sessions with a view of educating system users on preventing cyber-attacks to systems. 3.6.4 Apply various theories of privacy from a social psychology and social science in protecting system users' profiles. 3.6.5 Protect Sensitive Personal Data (SPD) and Personally Identifiable Information (PII) by applying relevant and appropriate measures.
3.7 Protect an organization from Cyber Security threats and manage risk to	3.7.1 Apply control risks measures to organizational information assets.

support the successful accomplishment of the organization's mission	3.7.2 Develop an information security policy for an organisation for use in managing system attacks 3.7.3 Align information security policy to be compliant with national and international laws and regulations, and specific industry standards. 3.7.4 Implement a Cyber Security system to circumvent intrusions.
3.8 Identify Laws, ethics, and policies vital to the security of corporate and government secrets and assets, as well as to the protection of individual privacy and identity.	3.8.1 Create measures to preserves the chain of digital evidence for use in prosecuting cybercrimes. 3.8.2 Comply with legal statutes on sections of the current legal environment in relation to cyberspace 3.8.3 Develop policies that encourage ethical use of ICT infrastructure in an organisation. 3.8.4 Review global impact of Cyber Security and how it influences culture and policy. 3.8.5 Apply practices and technologies used to safeguard personal privacy in an organisation.
3.9 Communicate succinctly to a range of audiences about multimedia software technical issues and their solutions	3.9.1. Document any proceeding of Information Technology Security using appropriate reporting format. 3.9.2. Write special documents on IT Security, taking into cognizance different report formats as per the scenario requires. 3.9.3. Apply relevant tools for creating software project reports 3.9.4. Present findings and observation to public gathering or one to one basis using appropriate tools for presentation. 3.9.5. Practice continuously both techniques of inter and intrapersonal communication skills to avoid misrepresentation and wrong conceptualization of discussions.
3.10 Manage one's own learning and development including management and organizational	3.10.1. Identify areas of weakness which need strengthen through staff development 3.10.2. Build capacity through subscription to recognized professional bodies and journals so as to be informed

skills for purposes of lifelong learning	dynamically of latest trends and developments in information security and emergent trends. 3.10.3. Organize and participate in Information Technology communities through social media platforms blog and presents on your self-reflection and perception on issues related to information security. 3.10.4. Collaborate with fellow information security experts from different institutions and organization with view to constructively create new knowledge and also share knowledge. 3.10.5. Subscribe to a professional body of information security.

4 QUALIFICATION STRUCTURESECTION C			
FUNDAMENTAL COMPONENT Subjects / Units / Modules /Courses	**Title**	**Level**	**Credits**
	Introduction to Computer Skills	5	15
	Creative and Innovation Studies	5	10
	Business Communication	5	10
	Computerized Mathematics	5	10
CORE COMPONENT Subjects / Units / Modules /Courses	Information Security Fundamentals	5	10
	Principles of Programming Logic & Design	5	10
	Introduction to Database Security	6	15
	Introduction to Data Communication	6	15
	Computer Organization and Architecture	6	10
	Web Systems and Technologies	6	15
	Introduction to Structured Programming	6	15
	Principles of Software Engineering	6	10
	Database Security	6	15
	Operating System	6	15
	Cryptography Fundamentals	6	15
	Introduction to Network Security	6	15
	Web Security	6	15

	Security Governance, Risk Management and Compliance	6	10
	Advanced Cryptography	6	10
	Advanced Programming in OOP	6	15
	Security Analytics	6	15
	Digital Forensics	7	10
	Network Security	7	15
	Data Structures and Algorithms	7	10
	Ethics and Professional Conduct	7	10
	Ethical Hacking	7	15
	Systems Analysis and Design	7	10
	Malware Analysis and Defense	7	10
	Network Penetration Testing	7	15
	Industrial Attachment	7	30
	IT Project Management	7	10
	Network Services Administration and Virtualization	7	15
	Business Information Security	7	15
	E-Commerce Systems	7	10
	Wireless and Mobile Networking	7	10
	Operations Security and Incident Management	7	10
	E-Commerce Security	7	10
	ICT Management and Strategy	7	10
ELECTIVE COMPONENT Subjects / Units / Modules /Courses	Cyber Terrorism & Cyber Warfare	8	15
	IT Security Management	8	15
	Information Security Audits	8	15
Total Credits			**500**

5 Rules of combinations, Credit distribution (where applicable):

5.1. Credit Award Rules

5.1.1. Qualification Bachelor of Science in Information Technology Security Credit Award Rules

Requirements for a learner to be awarded this qualification. The learner must accumulate a minimum of **500 credits** for them to be awarded the qualification. The order or requisite and prerequisite for the modules shall be followed

Compulsory Components Credits

- Complete Core modules with minimum of 440 Credits
- Fundamental modules with a minimum 45 Credits

Select Credits

- Elective modules 15 Credits

5.2. Qualification Bachelor of Sciencein information technology security Credit Distribution

Credit distributions for the qualifications are defined in consistence with the NCQF level 7 descriptors. The qualification bachelor's degree in information technology security is a four-year qualification program and students who undertake it shall complete a minimum of 500 credits distributed among 4 NCQF categories levels as follows

- Level 5 with a maximum of 65 credits,
- Level 6 with a minimum of 205 credits
- Level 7 with a maximum of 215 credits.
- Level 8 with a maximum of 15 credits

6 ASSESSMENT AND MODERATION ARRANGEMENTS

6.1 Assessment Arrangements

The qualification will encompass both formative and summative assessment, which will be designed by assessors who are BQA registered and accredited. The weightings for the assessments will be as follows;

Assessment Method	Weight (%)
Formative Assessments	60
Summative Assessments	40

6.2 Moderation Arrangements

- There will be internal and external moderation undertaken by moderators registered and accredited by BQA. All processes and procedures will be in line with NCQF requirements. This will be conducted in reference to the institution's moderation policy and procedures.

7 RECOGNITION OF PRIOR LEARNING (if applicable)

There will be provision of awarding the Bachelor of Science in Information Technology Security qualification through RPL according to the national RPL policy as per the NCQF requirements.

8 PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Horizontal articulation of Bachelor of ScienceInformation Technology Security

1. Bachelor's Degree in Computer Science
2. Bachelor's Degree in software engineering
3. Bachelor's Degree in information systems
4. Bachelor's Degree in information technology

Vertical Learning articulation of Bachelor of Sciencein Information Technology Security

1. Master of Science Computer Security
2. Master of Science Cyber Security
3. Master of Science in Cyber Security and Information Assurance

4 Master of Science in Computer Science (Cyber Security)

5 Master of Science in Security Risk Management

6 Master of Science in Digital Security

7 Master of Science in Information Security

Career Path in Information Technology Security

- IT Security Analyst.
- IT Security Engineer.
- IT Security Architect.
- IT Security Administrator.
- Security Software Developer.
- Software Security Engineer
- IT Security Consultant
- Information Security Officer
- Cryptographer.
- Cryptanalyst.
- ICT security Manager
- Data Centre Manager
- Computer Network Professionals
- Penetration and Vulnerability Tester
- Forensic specialists (ICT)

9 QUALIFICATION AWARD AND CERTIFICATION

9.1 Minimum standards of achievement for the award of the qualification

The Qualification is **Bachelor of Science in Information Technology Security** is only awarded to learners who have completed and attained all the requirements of the programme as follows.

- Have official verification that (s)he has covered and passed all the modules in the qualification
- Has completed a minimum of **500 credits** overall.

10 REGIONAL AND INTERNATIONAL COMPARABILITY

The international and regional comparability looked at the following attributes

(a) Exit outcomes
(b) Duration
(c) Minimum qualification Credits offered and level of qualification descriptor based on country NCFQ
(d) Elective availability
(e) Content

10.1 Regional Comparability

There are very few institutions offering the qualification Information Technology Cyber Security I regional and in Africa**.** Only two institutions were used for regional comparative analyses. One qualification in Namibia and the other in Nigeria.

Criteria	Federal University of Technology, Minna (Nigeria)	Namibia University (Namibia)
Degree Programme	BSc Cyber Security Bachelor	BSc Computer Science in Cyber Security
Exit Learning Outcome	▪ Describe major components of a corporate IT infrastructure. ▪ Identify the standards and technologies in networking and security that support making informed business decisions. ▪ Compare and contrast technologies in networking and security designed to solve similar problems. ▪ Defend IT and security recommendations for business solutions. ▪ Communicate effectively with both verbal and written forms ▪ Install, configure, use, and manage anti malware software on a working network ▪ Evaluate best practices in security concepts to maintain confidentiality, integrity, and availability of computer systems	▪ Analyse a problem and design the cybersecurity measures appropriate to its solution. ▪ Apply concepts of best practices in cybersecurity management to enterprise processes. ▪ Describe the ethical challenges that confront a cybersecurity professional. ▪ Apply security control principles in the construction of cybersecurity solutions. ▪ Demonstrate written and oral communication skills. ▪ Demonstrate the ability to securely administer a Windows and Linux system ▪ using security automation tools and techniques. ▪ Demonstrate knowledge of the fundamental concepts of operating systems, ▪ networks, and cloud computing.
Programme Duration	4 years programme	3 years programme
Credits Awarded	NSQ Level 5 (Nigerian – NSQF)	Level 7. Minimum 480 credits (Namibian NQF)
Electives Modules	Does not have elective	Does not have electives

Work Placement	Students are not attached	Internship i.e., industrial attachment
Content Coverage	Content coverage correspond to 70%	Content coverage correspond to 75%
Assessment Strategies	Practical, theoretical, Project, Group Work, Examinations, Computer Labs Practice, Test, Presentations, prototypes	Practical, theoretical, work attachment, Project, Group Work, Examinations, Computer Labs Practice, Test, Presentations, prototypes

Similarities Analysis: All qualifications have assessments strategies which include key strategies like projects, internship, workshop practice, theoretical evaluations and group works. **Conceptually** the learning outcomes tend to cover key domain areas like communication skills, teamwork skills, computer literacy skills, information security, cyber security, and the theoretical and technical background of the domain of study. There is an average of 87% in content coverage when compared with Qualification in Information Technology Cyber Security. Empirical rating makes the qualification portable and generalizable with regional courses. All qualifications are based on their respective National Qualification Frameworks.

Differences Analysis: All qualifications are placed at different levels according to the respective National Qualification Framework. The qualification in Nigerian uses level 5, but the Namibian qualification uses level 7. Titles of the qualifications vary but they deliver almost the same content. The Qualification Information Technology Cyber Security offers industrial attachment, but qualification Cyber Security does not. The qualification Computer Science in Cyber Security from Namibia offers attachment, and this is tandem with the qualification Information Technology Cyber Security. The qualification Information Technology Cyber Security offers electives and others do not.

Contextualization Analysis: In context of Botswana, the Qualification Information Technology Cyber Security offers industrial attachment within course and has a project work at the end of the qualification. The qualification also offers electives as a way to enhance and promote specialisation. The qualification is placed at level 7 in tandem with many qualifications at general degree level inclusive the Namibian qualification.

10.2 International Comparability

Criteria	DeVary University	Educational and Research Institute	Royal Holloway University of London	Hongyi Wu, Program Coordinator and
Degree Programme	Information Technology and Networking (Cyber Security)	Bachelor of Technology - Information Security and Digital Forensics	BSc Computer Science (Information Security)	Bachelor of Science in Cyber security
Exit Learning Outcome	• Apply concept of confidentiality, availability, and integrity (CIA) in context of Information Security • Configure host and network level technical security controls • Identify hardware, software, and services that comprise an enterprise network • Build multi-host and network architectures given business requirements • Effectively Communicate • Serve as contributing member of small to large projects	• Determine factors driving the need for network security • Classify particular examples of attacks • Define the terms vulnerability, threat, and attack • identify physical points of vulnerability in simple networks • compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems	• Analyse a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions. • Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline. • Communicate effectively in a variety of professional contexts. • Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles. • Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline. • Identify and analyse user needs and to take them into account in the selection, creation, integration, evaluation,	• Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure. • Design, develop, test, and evaluate secure software. • Develop policies and procedures to manage enterprise security risks. • Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training. • Interpret and forensically investigate security incidents.

			and administration of computing-based system	
Programme Duration	3 years programme	3 years programme	4-year programme	4-year programme
Credits Awarded	121 credits. No use of National Qualifications	184 Credits	Level 6 qualification. minimum 360 credits UK (FHEQ)	120 Credits
Electives Modules	Does not have elective	Does not have electives	Has electives	Does not have electives
Work Placement	Students are not attached for internship	Has project work & Internship	Has project work & Internship	Has project work & Internship
Content Coverage	Content coverage correspond to 70%	Content Coverage correspond to 100%	Content coverage correspond to 95%	Content coverage correspond to 80%
Assessment Strategies	Practical, theoretical, work attachment, Project, Group Work, Examinations, Computer Labs Practice Test, Presentations, prototypes	Practical, theoretical, work attachment, Project, Group Work, Examinations, Computer Labs Practice Test, Presentations, prototypes	Practical, theoretical, work attachment, Project, Group Work, Examinations, Computer Labs Practice Test, Presentations, prototypes	Practical, theoretical, work attachment, Project, Group Work, Examinations, Computer Labs Practice Test, Presentations, prototypes

Similarities Analysis: About 90% of the institutes ran the qualification on minimum of 3 years duration. **All** qualifications are based on national qualification framework except the USA. The USA qualification is mostly driven by professional bodies and accreditation. **All** qualifications have assessments strategies which include projects, internship, workshop practice, theoretical evaluations and group works.

Differences Analysis: The qualifications have different names but the content and concept is convergent. A majority of the qualifications are also accredited with the professional bodies. A minority of the qualifications do not offer electives. A majority of the qualifications still use the 1-hour credit notion.

Contextualization Analysis: In context of Botswana Qualification Information Technology Cyber Security, it uses the 10 hours notional credit systems. It has also adopted Internship and group projects. It will cover duration of 4 years.

International Qualification Portability and Generalisation: The qualification is generally compatible and compliant to the qualifications sampled in the international arena

11 REVIEW PERIOD

The period for reviewing the Qualification Bachelor of Science in Information Technology Security is after five (5) years.

12 Other information – please add any supplementary information to help the application for this qualification for NCQF Registration.

Following Information have been used for references please find attached

1. Needs Analysis Document
2. HRDC Document
3. Ministry of Transport and Communication Report: National Strategy on Cyber Security.
4. National Development Plan 10 and 11
5. Maitlamo National ICT Policy.
6. Newspaper Editorial Articles