BQA NCQF QUALIFICATION TEMPLATE

SECTION A:	QUALIFICATION DETAILS
QUALIFICATION DEVELOPER (S)	Rankuke Training Institute

TITLE	Diploma in Digital Security	**NCQF LEVEL**	6
STRANDS (where applicable)	a) Diploma in Digital Security in Cybersecurity b) Diploma in Digital Security in Forensic Investigation		
FIELD	Law and Security	**CREDIT VALUE**	360
SUB FIELD	Security		

New Qualification	✓	Legacy Qualification		Renewal Qualification	
				Registration Code	

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:

Botswana's rapid digitalization across government, finance, telecommunications, and education has increased exposure to cybercrime, data breaches, and technology-enabled offences. This has created an urgent need for professionals with specialized skills in cybersecurity, digital forensics, and cyber-risk management. The 2025 HRDC Skills Report identifies future digital skills as a national priority, emphasizing cybersecurity and forensic capabilities as essential for supporting the digital economy and the Fourth Industrial Revolution.

Botswana has strengthened its regulatory environment through the Cybercrime and Computer Related Crimes Act, enhancing the country's ability to prevent, detect, investigate, and prosecute cyber offences. Combined with the Forensic Procedures Act (2014), this reinforces the need for practitioners with both technical and investigative expertise to address increasingly complex crimes.

This integrated Diploma equips learners with practical competencies in cyber defense, digital evidence handling, and investigative procedures, supporting justice processes, enhancing national security, and strengthening Botswana's overall digital resilience.

The module "Basic Computing and Networking" is positioned at NCQF Level 5 to provide foundational digital literacy and introductory networking competencies for learners who may not have prior formal exposure to computing studies at secondary level. This bridging approach supports inclusive access while ensuring that all learners are adequately prepared to engage with higher-level cybersecurity and digital forensic modules delivered at NCQF Level 6. The module therefore functions as an academic progression enabler rather than a core specialised competency.

Artificial Intelligence is incorporated within the qualification from a cybersecurity risk-impact perspective rather than a programming depth, ensuring that learners develop the ability to assess, manage, and respond to AI-related risks within organisational and security environments.

This qualification aligns with Botswana's cybercrime legislation, digital evidence requirements and data protection obligations. It also aligns to the NCQF Level 6 Descriptors, which require applied technical competence, analytical problem-solving, supervised autonomy, and the ability to apply theoretical knowledge to occupational contexts in cybersecurity and forensic investigation.

PURPOSE:

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

1. Apply cybersecurity principles, tools, and techniques in accordance with recognised frameworks (e.g., ISO 27001, NIST) and organisational policies to protect digital systems, networks, and information assets, and analyse cyber risks through structured testing using established risk assessment and vulnerability management methodologies within organisational contexts.
2. Conduct digital and cybercrime investigations using recognised forensic methodologies, tools, and procedures, and collect, preserve, analyse, and present digital and physical evidence in accordance with chain-of-custody requirements, forensic standards, and legal frameworks to ensure evidentiary integrity and admissibility.
3. Interpret and apply cybersecurity, data protection, and cybercrime laws, policies, and regulatory frameworks, aligned to national legislation and international standards, to ensure legal compliance and responsible conduct in cybersecurity and digital forensic environments.
4. Perform specialised digital, mobile, and financial forensic analysis using advanced tools and investigative frameworks to identify, correlate, and interpret digital evidence in complex investigative scenarios.
5. Respond to cybersecurity incidents by applying recognised incident response frameworks and organisational procedures, including detection, containment, eradication, recovery, and reporting, to minimise impact and restore system integrity.
6. Communicate cybersecurity and forensic findings using professional reporting standards and

stakeholder engagement practices, while demonstrating ethical conduct, professional judgement, and adherence to recognised codes, standards, and regulatory requirements in all cybersecurity and forensic activities.

Stakeholder Consultation and Industry Validation

The development of the Diploma in Digital Security (Cybersecurity or Forensic Investigation) involved consultation with relevant stakeholders in the information and communications technology (ICT), cybersecurity, digital forensics, financial services, law enforcement, and regulatory compliance sectors to ensure that the qualification reflects current professional practice, regulatory expectations, and labour market needs within Botswana's digital economy and national security landscape.

Key stakeholders consulted during the qualification design process included cybersecurity practitioners, digital forensic investigators, ICT governance specialists, financial sector compliance professionals, law enforcement personnel, and technology service providers. The consultation process focused on identifying competency requirements for mid-level practitioners responsible for cybersecurity risk management, incident response, digital evidence handling, regulatory compliance, and the protection of organisational information systems.

Stakeholder feedback emphasized the need for graduates who possess practical competencies in cybersecurity operations, network defence, cyber incident investigation, digital forensic analysis, information security governance, and compliance with relevant legal and regulatory frameworks. Stakeholders also highlighted the importance of integrating laboratory-based learning, real-world case studies, and structured workplace exposure to ensure that graduates can function effectively in operational cybersecurity and investigative environments.

In response, the qualification incorporates applied assessment methodologies, competency-based learning approaches, and a structured Work-Integrated Learning (WIL) component to ensure alignment between academic preparation and industry practice. The qualification integrates foundational knowledge in information security principles, digital forensic methodologies, cyber law, and governance frameworks to support effective professional practice in cybersecurity and digital investigations.

The developed qualification aligns with national workforce development priorities identified by the Human Resource Development Council (HRDC) and contributes to capacity development within government ICT units, financial institutions, telecommunications companies, cybersecurity service providers, regulatory bodies, and law enforcement agencies involved in cybercrime prevention and investigation.

This stakeholder-informed approach ensures that the qualification remains responsive to sector expectations and contributes to the development of a competent workforce capable of strengthening cybersecurity resilience, digital governance, and investigative capacity within Botswana.

Labour Market Demand Evidence

The demand for skilled cybersecurity and digital forensic practitioners in Botswana continues to increase as organisations across both public and private sectors expand their reliance on digital systems, electronic transactions, and networked technologies. The growth of digital services, financial technology platforms,

and e-government initiatives has heightened exposure to cyber threats, data breaches, and technology-enabled financial crimes.

The Human Resource Development Council (HRDC) has identified digital and ICT-related competencies as critical priority skills required to support Botswana's transition toward a knowledge-based and digitally enabled economy. Organisations face increasing challenges in securing information infrastructure, managing cyber risk, responding to security incidents, and ensuring compliance with evolving regulatory requirements related to data protection, cybersecurity governance, and digital evidence management.

Furthermore, Botswana's strengthening of legal and regulatory frameworks addressing cybercrime, electronic transactions, and data protection has increased the need for professionals capable of conducting digital investigations, supporting forensic analysis, and implementing cybersecurity controls aligned to national and international standards.

Institutions such as government ministries, law enforcement agencies, financial institutions, telecommunications providers, technology companies, and cybersecurity consulting firms require personnel with specialised competencies in cybersecurity operations, digital forensic investigation, information security governance, and cyber risk management.

The proposed Diploma in Digital Security (Cybersecurity or Forensic Investigation) therefore responds directly to these labour market needs by developing graduates with applied competencies in cybersecurity defence, digital investigation, regulatory compliance, and information security management. By strengthening local technical capacity in these areas, the qualification contributes to Botswana's broader national objectives of enhancing digital resilience, protecting critical information infrastructure, and supporting effective cybercrime prevention and response mechanisms.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

Minimum Entry Requirements:
NCQF Level 4 qualification (e.g., BGCSE or equivalent).

Recognition of Prior Learning (RPL):
RPL may be applied in accordance with institutional and national frameworks.

SECTION B	QUALIFICATION SPECIFICATION
GRADUATE PROFILE (LEARNING OUTCOMES)	***ASSESSMENT CRITERIA***
LO1: Apply cybersecurity principles, tools, and techniques in accordance with recognised cybersecurity frameworks (e.g., ISO 27001, NIST) and organisational security policies to protect digital systems, networks, and information assets in operational and investigative environments.	1.1 Configure and implement basic and intermediate security controls on operating systems, networks, and applications in accordance with recognised cybersecurity frameworks (e.g., ISO 27001, NIST) and organisational security policies, to protect information systems in real or simulated environments. 1.2 Identify common vulnerabilities using recognised vulnerability-scanning tools and techniques by applying vulnerability assessment frameworks and industry-standard tools (e.g., Nessus, OpenVAS), to detect weaknesses in systems and networks within controlled or operational environments. 1.3 Evaluate system configurations against established security baselines and standards, such as CIS benchmarks and organisational configuration standards, to assess compliance and identify security gaps in system environments. 1.4 Demonstrate secure-by-design and defence-in-depth principles in laboratory simulations by applying security architecture frameworks and layered security models, to design and implement resilient cybersecurity solutions. 1.5 Produce a technical report outlining identified risks and recommended remediation measures by applying professional reporting standards, risk assessment frameworks, and organisational documentation procedures, to support decision-making and regulatory compliance.
LO2: Analyse cyber risks and conduct structured security testing by applying risk assessment frameworks, penetration testing methodologies, and vulnerability management standards, to identify threats, vulnerabilities, and appropriate mitigation strategies within organisational contexts.	2.1 Conduct qualitative and quantitative risk assessments using recognised risk frameworks (e.g., ISO 27005, NIST Risk Management Framework) within organisational or simulated environments, to identify, analyse, and evaluate cybersecurity

	risks affecting information systems and operations. 2.2 Perform controlled penetration testing and ethical hacking exercises by applying industry-standard methodologies (e.g., OWASP Testing Guide, penetration testing frameworks) within defined legal, ethical, and institutional boundaries, to identify exploitable vulnerabilities in systems and networks. 2.3 Interpret test results and prioritise vulnerabilities based on severity and likelihood by applying risk rating models (e.g., CVSS scoring) and vulnerability management frameworks, to support effective remediation and risk management decisions. 2.4 Develop practical mitigation and risk-treatment plans by applying risk management strategies, security control frameworks, and organisational policies, to reduce identified risks and enhance system security and resilience. 2.5 Present risk findings using professional documentation standards by preparing structured risk assessment and penetration testing reports in accordance with organisational reporting procedures and regulatory expectations, to support stakeholder decision-making and compliance
LO3: Conduct digital and cybercrime investigations using recognised forensic methodologies, investigative procedures, and digital forensic tools, in accordance with legal and evidentiary requirements, to support incident analysis and prosecution processes.	3.1 Acquire and preserve digital evidence using accepted forensic imaging techniques (e.g., disk imaging and write-blocking) in accordance with recognised forensic standards and evidentiary procedures, to ensure integrity and admissibility in investigative contexts. 3.2 Apply recognised investigative methodologies (e.g., digital forensic process models) to reconstruct incident timelines within real or simulated cyber incident environments, to support accurate event analysis. 3.3 Utilise forensic software tools (e.g., EnCase, FTK, Autopsy) to analyse file systems, logs, and artefacts in controlled laboratory or operational environments, to extract and interpret digital evidence. 3.4 Distinguish between different categories of cyber incidents by applying incident classification frameworks and threat models, to select appropriate investigative

	approaches in organisational or simulated contexts. 3.5 Document investigative processes in accordance with evidentiary standards, organisational procedures, and legal requirements, to ensure traceability and admissibility of findings.
LO4: Collect, preserve, analyse, and present digital and physical evidence in accordance with chain-of-custody procedures, forensic standards, and applicable legal and ethical frameworks, to ensure integrity, admissibility, and reliability of evidence in investigative contexts.	4.1 Demonstrate correct chain-of-custody procedures and evidence-handling protocols in accordance with forensic standards and legal requirements, to maintain integrity and admissibility of evidence. 4.2 Maintain accurate documentation and audit trails throughout the investigation lifecycle using forensic documentation standards and organisational procedures, to support accountability and traceability. 4.3 Produce legally defensible forensic artefacts and analytical summaries by applying evidentiary standards and reporting frameworks, to support legal and regulatory processes. 4.4 Apply national legislation and procedural requirements (e.g., cybercrime and evidence laws) to evidence collection scenarios, to ensure compliance in investigative contexts. 4.5 Justify evidence-handling decisions by applying ethical principles, professional standards, and legal frameworks, to support defensible investigative outcomes.
LO5: Interpret and apply relevant cybersecurity, data protection, and cybercrime laws, policies, and regulatory frameworks by referencing national legislation and international standards, to ensure legal compliance and responsible conduct in cybersecurity and digital investigation environments.	5.1 Identify applicable national and international legal and regulatory instruments governing cybersecurity and digital investigations by referencing relevant legislation, standards, and policies, to support compliance. 5.2 Apply legal provisions to simulated investigative and organisational scenarios in accordance with statutory requirements and regulatory frameworks, to ensure lawful practice. 5.3 Evaluate organisational compliance with data protection and cybersecurity obligations by applying compliance frameworks and regulatory standards, to identify gaps and risks. 5.4 Analyse the legal implications of investigative actions and system monitoring activities by applying legal interpretation principles and

	regulatory guidelines, to support lawful decision-making. 5.5 Demonstrate awareness of privacy, confidentiality, and due-process considerations in accordance with data protection laws and ethical standards, to ensure responsible practice.
LO6: Perform specialised digital, mobile, and financial crime forensic analysis using advanced forensic tools, analytical techniques, and investigative frameworks, to identify, interpret, and correlate digital evidence in complex investigative scenarios.	6.1 Extract and analyse data from computers, mobile devices, and removable media using specialised forensic tools in controlled laboratory or investigative environments, to identify relevant evidence. 6.2 Conduct malware behaviour analysis in a controlled laboratory environment using recognised analytical frameworks and sandboxing techniques, to understand threats and system impact. 6.3 Apply basic forensic accounting and financial transaction analysis techniques in fraud investigations by using analytical tools and financial investigation frameworks, to detect irregularities. 6.4 Correlate digital artefacts by applying forensic analysis methodologies and data correlation techniques, to establish patterns of activity and intent. 6.5 Produce structured analytical findings supported by verifiable digital evidence in accordance with forensic reporting standards and organisational requirements, to support investigations.
LO7: Respond effectively to cybersecurity incidents by applying incident response frameworks, organisational procedures, and industry best practices, including detection, containment, eradication, recovery, and reporting, to minimise impact and restore system integrity.	7.1 Detect and interpret security alerts, anomalies, and indicators of compromise by applying monitoring tools and threat detection frameworks, to identify cybersecurity incidents. 7.2 Apply incident-response frameworks (e.g., NIST IR framework) and escalation protocols in simulated or organisational environments, to manage incidents effectively. 7.3 Coordinate response actions, including containment and system recovery, by applying organisational procedures and best practice frameworks, to minimise operational impact. 7.4 Maintain incident logs and communication records in accordance with incident

	management standards and organisational requirements, to ensure traceability. 7.5 Compile structured incident-response reports with actionable recommendations using professional reporting standards, to support decision-making and compliance.
LO8: Communicate cybersecurity and forensic findings by applying professional communication standards, reporting frameworks, and stakeholder engagement practices, to present technical and investigative information clearly to both technical and non-technical audiences.	8.1 Produce structured investigative and technical reports using accepted professional and forensic reporting standards, to communicate findings effectively. 8.2 Present analytical findings verbally using professional communication frameworks and evidence-based reasoning, to support stakeholder understanding. 8.3 Translate technical terminology into language understandable to non-technical audiences by applying communication best practices, to enhance accessibility. 8.4 Support conclusions with credible data, visualisations, and referenced artefacts in accordance with reporting and evidentiary standards, to ensure validity. 8.5 Demonstrate accuracy, clarity, and objectivity in all forms of communication by adhering to professional and organisational standards, to maintain credibility.
LO9: Demonstrate ethical conduct and professional judgement by adhering to recognised ethical codes, professional standards, and regulatory requirements, to ensure integrity, accountability, and responsible practice in cybersecurity and forensic work.	9.1 Apply ethical principles and professional codes of conduct in decision-making scenarios by adhering to recognised cybersecurity and forensic ethical standards, to ensure integrity. 9.2 Demonstrate integrity, confidentiality, and responsible use of investigative and security tools in accordance with organisational policies and legal requirements, to ensure responsible practice. 9.3 Recognise and resolve ethical dilemmas in simulated occupational contexts by applying ethical decision-making frameworks, to support professional judgement. 9.4 Comply with institutional, national, and international standards governing cybersecurity and forensic activities, to ensure regulatory and professional compliance. 9.5 Reflect critically on personal performance and professional responsibilities by applying

	reflective practice frameworks, to support continuous professional development.

SECTION C	QUALIFICATION STRUCTURE One credit represents 10 notional learning hours.				
COMPONENT	TITLE	Credits Per Relevant NCQF Level			Total Credits
		Level [5]	Level [6]	Level [7]	
FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Professional Communication in Cybersecurity	10			10
	Digital Innovation & Cybersecurity Services	10			10
	Employability and Professional Practice	10			10
	Environmental Sustainability	10			10
	Cyber Lab & Data Centre Safety	10			10
	Basic Computing and Networking	10			10
	TOTAL CREDITS				**60**
CORE COMPONENT Subjects/Courses/ Modules/Units	Introduction To Forensic Science and Criminal Investigation		10		10
	Criminal Law		10		10
	Cybersecurity Fundamentals		10		10
	Data Protection and Privacy		10		10
	Artificial Intelligence and Cyber Impact		10		10
	Computer Networking		12		12
	Secure Network Design		11		11
	Cyber Risk Assessment & Testing		12		12
	Physical Evidence Collection & Preservation		12		12
	Incident Investigation			12	12
	Cyber Crime and Digital Investigation		11		11

	Malware Analysis Tools & Techniques		10		10
	Cyber Governance, Risk and Compliance		10		10
	Cyber Laws, Policies & Regulations		10		10
	Forensic Science Principles & Techniques		12		12
WORK-INTEGRATED LEARNING	Supervised Industrial Attachment (minimum 20-24 weeks) **OR** Project Report (where workplace placement is not feasible)		60		60
	TOTAL CREDITS				**222**

STRANDS/ SPECIALIZATION *(must select one strand)*	Subjects/ Courses/ Modules/Units	**Credits Per Relevant NCQF Level**			**Total Credits**
		Level [ ]	**Level [6]**	**Level [ ]**	
1. CYBERSECURITY	Cybersecurity Operations & Threat Intelligence		12		12
	Ethical Hacking		12		12
	Network Security		10		10
	Incident Handling		12		12
	Digital Incident Forensics		10		10
	Advanced Penetration Testing Project		12		12
	Security Operations Lab		12		12
	TOTAL CREDITS				**78**
2.FORENSIC INVESTIGATION	Computer and Digital Forensics		10		10
	Forensic Investigation Report Writing and Communication		10		10
	Frauds and Financial Crime Forensics		12		12
	Digital and Mobile Forensics Investigations		11		11

	Advanced Evidence Analysis Project		12		12
	Courtroom Testimony Simulation		11		11
	Forensic Lab Practicum		12		12
	TOTAL CREDITS				**78**

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	**Credit Value**
5	60
6	288
7	12
TOTAL CREDITS	**360**

Rules of Combination: **(Please Indicate combinations for the different constituent components of the qualification)**
To be awarded the qualification, learners must complete all fundamental and core modules, one specialisation pathway accumulate a total of 360 credits.

ASSESSMENT ARRANGEMENTS
Assessment will comprise formative (70%) and summative (30%) components in line with competency-based education principles. Assessment will be conducted in accordance with the institution's approved assessment and moderation policy.

Assessors will possess relevant academic and/or professional qualifications at a minimum of one level above the qualification, with appropriate industry experience.

Both internal and external moderation will be applied to ensure validity, reliability, and consistency of assessment decisions

PASS REQUIREMENTS

Minimum weighted pass mark of 60% per module.

MODERATION ARRANGEMENTS

Moderation will be conducted in accordance with the institution's approved assessment and moderation policy. Both internal and external moderation will be applied to ensure validity, reliability, fairness and consistency of assessment decisions.

Moderators will possess relevant academic and/or professional qualifications at a minimum of one level above the qualification, with appropriate industry experience.

RECOGNITION OF PRIOR LEARNING

Recognition of Prior Learning (RPL) for access and/or credit may be applied in accordance with institutional policy and national guidelines.

CREDIT ACCUMULATION AND TRANSFER

Credit Accumulation and Transfer (CAT) may be applied in accordance with institutional and national frameworks.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Horizontal Articulation (related qualifications of similar level that graduates may consider):
Graduates may consider related qualifications of a similar level, such as:

- Diploma in Information Technology
- Diploma in Network Administration
- Diploma in Computer Systems Engineering
- Diploma in Criminal Justice or Policing or Digital Forensics
- Diploma in Data Analytics or Information Systems

Vertical Articulation (pathways which the holders may progress to):
Graduates may progress to higher qualifications, such as:

- Bachelor's Degree in Cybersecurity
- Bachelor's degree in Digital Forensics
- Bachelor's degree in Computer Science or Information Technology
- Bachelor's degree in Criminal Justice, Criminology, or Forensic Science
- Bachelor's degree in information systems, Data Science, or Software Engineering
- Bachelor of Technology in Forensic and Criminal Investigation

Employment Pathways:
Graduates are equipped for roles in cybersecurity, digital forensics, ICT security operations, and regulatory environments, across both private sector (ICT security, consulting) and public sector (law enforcement, regulatory, and national security) organisations. They can pursue various roles in the field, such as:

- Cybersecurity Technician
- Cybersecurity Officer
- Digital Forensics Technician
- Digital Forensic Analyst
- Cybercrime Investigator
- Incident Response Analyst
- Network Security Technician
- Cyber Governance, Risk and Compliance Assistant
- Malware Analyst (Entry-Level)
- Fraud and Financial Crime Forensics Assistant
- IT Support Technician (Cybersecurity Focus)
- Mobile Forensics Assistant
- Computer Forensics Assistant

QUALIFICATION AWARD AND CERTIFICATION

To be awarded the Diploma in Digital Security (Cybersecurity/ Forensic Investigation), a learner must successfully complete a total of 360 credits.

The institution will issue an official certificate and academic transcript upon completion.

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

Introduction

Graduates of this qualification will possess advanced knowledge, practical skills, and professional competence to secure digital systems, conduct cybersecurity operations, and perform digital forensic investigations in accordance with applicable legal, regulatory, and professional frameworks. They will be able to manage cyber risks, respond to security incidents, analyse digital evidence, and apply innovative and technology-driven solutions within cybersecurity and forensic environments. Graduates will demonstrate ethical conduct, accountability, and professional judgement in cybersecurity and digital forensic practice.

In addition, graduates will demonstrate:

- **Knowledge:** Advanced theoretical and practical knowledge of cybersecurity principles, digital forensic methodologies, information security governance, cyber risk management, and applicable legal and regulatory frameworks.
- **Skills:** Cognitive, analytical, and technical skills to identify and mitigate cyber threats, conduct forensic investigations, analyse digital evidence, and apply cybersecurity tools and investigative techniques to solve complex security and forensic challenges.
- **Responsibility and Autonomy:** Ability to operate independently within cybersecurity and forensic environments, exercise professional judgement, adhere to ethical and legal standards, and take responsibility for decisions related to cybersecurity operations, incident response, and digital investigations.

A comparative analysis of the developed qualification was undertaken against three (3) similar and equivalent qualifications from both regional and international learning institutions to determine parity of level, breadth of content, delivery approaches, and assessment structures. The developed qualification was benchmarked against the Diploma in Forensic and Criminal Investigation offered by the National Institute of Technology (NIT) in Namibia, the Diploma in Cybersecurity and Forensics offered by Zetech University in Kenya, and the Diploma in Cybersecurity & Digital Forensics offered by Ngee Ann Polytechnic in Singapore. The analysis focused on qualification level, duration, curriculum scope, practical intensity, assessment methodology, and work-integrated learning requirements.

Similarities and Differences Observed

The benchmarking exercise demonstrates substantial similarities between the developed qualification and comparable regional and international programmes. All qualifications include core subject areas such as cybersecurity fundamentals, networking, digital forensics, ethical hacking, and cyber law, while placing significant emphasis on practical, hands-on learning through laboratory work, simulations, projects, and applied assessments. Assessment approaches across the benchmarked programmes combine continuous assessment with examinations and practical evaluations, and all provide clear progression pathways into bachelor's degree programmes in cybersecurity, digital forensics, information technology, and related disciplines. Employment outcomes are similarly aligned, preparing graduates for entry-level cybersecurity and digital forensic roles.

The developed qualification is distinguished by several unique features. It introduces Artificial Intelligence from a cybersecurity risk and impact perspective rather than as a programming specialisation and offers two specialist pathways in Cybersecurity and Forensic Investigation, allowing for deeper specialisation than most comparator programmes. Its 360-credit structure provides broader coverage through enhanced laboratory training, dual specialisation pathways, and a compulsory 60-credit Work Integrated Learning (WIL) component that exceeds the internship requirements of most benchmark institutions.

While some international programmes include specialised areas such as Cloud Security, Operational Technology (OT) Security, entrepreneurship, research methods, and cloud computing, the developed qualification adopts a competency-based assessment model comprising 70% formative and 30% summative assessment, reflecting its strong practical, laboratory-intensive, and investigative orientation.

Overall Comparability Conclusion

Across the three institutions, common areas of convergence include cybersecurity fundamentals, digital forensics, incident response, ethical hacking, governance and compliance, and practical laboratory exposure. The principal differences lie in qualification duration, credit weighting, and the explicit structuring of workplace learning components. The developed qualification demonstrates equivalent academic depth and occupational relevance to regional and international diploma standards while maintaining contextual alignment with Botswana's legal framework, regulatory environment, and labor-market requirements. This positioning confirms that the developed qualification is comparable in level, scope, and applied intensity to established cybersecurity and digital forensics diplomas internationally.

REVIEW PERIOD

The Diploma in Digital Security (Cybersecurity or Forensic Investigation) shall be reviewed every five (5) years.

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**	