BQA NCQF QUALIFICATION TEMPLATE

SECTION A:	QUALIFICATION DETAILS												
QUALIFICATION DEVELOPER (S)	**Cyber Intelligence College (CIC) Botswana**												
TITLE	Bachelor of Science in Enterprise Security Architecture (BSc ESA)							**NCQF LEVEL**	7				
STRANDS (where applicable)	N/A												
FIELD	Information and Communications Technology							**CREDIT VALUE**	480				
SUB FIELD	Information Technology												
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:

This qualification addresses Botswana's critical need for expertise in enterprise security architecture amid digital transformation, with global cyber threats escalating at 921 password attacks per second and a projected 32% job growth for security analysts through 2032 (BLS

2023, median salary $120,360). It aligns with Botswana's Vision 2036 (Pillars 1 and 2) for sustainable development, NDP 11's knowledge-based economy, the Botswana Cybersecurity Act (2024) for national security, the National Cybersecurity Strategy for threat mitigation, and the EU Digital Services Act for compliance in digital service development. Informed by CIC's 2025 Enterprise Security Needs Assessment Survey and HRDC Priority Skills 2023/2024 (cybersecurity, risk management, digital services), it fills skills gaps in secure architecture and governance. Benchmarking University of Maryland's cybersecurity specialization (US, cloud security focus), Carnegie Mellon's secure software (US), Stanford's cloud innovation (US), Georgia Tech's enterprise focus (US), ETH Zurich's architecture research (Switzerland), University of Warwick's NCSC-certified Cyber Security (UK), University of Oxford's cybersecurity pathway (UK), University College London's enterprise security (UK), Manchester Metropolitan University's DevSecOps/cloud emphasis (UK), University of Cape Town's cybersecurity (Africa), University of Pretoria's information systems (Africa), and BIUST's Cyber Security (Africa), the program embeds certifications (e.g., TOGAF, CEH, CISSP, AWS Certified Security) and real-world projects to produce graduates who innovate resilient architectures and compete globally.

PURPOSE (itemise exit level outcomes):

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

1. Design, develop, and govern a robust enterprise security architecture that holistically addresses an organisation's business requirements and risk landscape to create blueprints for secure, compliant, and resilient IT infrastructure.
2. Apply advanced cybersecurity principles and techniques to secure modern technological ecosystems, including cloud platforms, the Internet of Things (IoT) devices, and AI-driven systems.
3. Perform and lead comprehensive risk assessments and implement robust cybersecurity governance programs to enable effective risk mitigation and regulatory compliance
4. Lead and execute proactive threat intelligence and ethical hacking operations to discover and evaluate vulnerabilities, anticipate threats, and harden enterprise defences.

5. Integrate DevSecOps principles and security automation into the software development lifecycle to build and maintain resilient and secure infrastructure.
6. Communicate complex cybersecurity strategies, risks, and solutions to influence security investment decisions, and lead enterprise-wide security initiatives.

MINIMUM ENTRY REQUIREMENTS (including access and inclusion)

1. Applicants must have a minimum of Certificate IV, NCQF Level 4 (TVET/GE) or equivalent
2. Candidates who do not meet the minimum academic qualifications stated above will be considered through the Recognition of Prior Learning (RPL) process which shall be administered according to the National RPL Policy. There will also be provision for Credit Accumulation Transfer to the learner in case they transfer in from another institution as per National Policy on CAT.

SECTION B	QUALIFICATION SPECIFICATION
GRADUATE PROFILE (LEARNING OUTCOMES)	**ASSESSMENT CRITERIA**
1. Design and model enterprise-wide security architectures for complex, multi-faceted organizations using industry-standard frameworks like TOGAF and SABSA.	1.1 Analyse organizational structures, processes, and information flows to identify security requirements across business, information, application, and technology domains. 1.2 Develop security architecture models and blueprints using TOGAF and SABSA methodologies that align with organizational strategy and regulatory compliance needs.

	1.3 Integrate security principles into enterprise architecture layers to ensure interoperability, scalability, and resilience in complex environments. 1.4 Evaluate architectural designs through simulation, scenario testing, and peer review to validate effectiveness against threats and organisational objectives.
2. Design and implement robust security controls for dynamic cloud, microservices, and virtualised infrastructures to protect against evolving threats.	2.1 Implement automated monitoring and logging solutions that detect, alert, and respond to suspicious activities in dynamic infrastructures. 2.2 Apply secure configuration and deployment practices (e.g., container hardening, zero-trust principles, least privilege) to safeguard against misconfigurations and vulnerabilities. 2.3 Evaluate and validate security controls through penetration testing, threat modelling, and compliance assessments to ensure resilience against evolving cyber threats.
3. Evaluate and secure emerging technologies, such as IoT and AI systems, by integrating advanced cybersecurity techniques and security-by-design principles.	3.1 Assess vulnerabilities and risks specific to IoT and AI systems by applying threat modelling and risk evaluation methodologies. 3.2 Design security-by-design architectures that integrate privacy, resilience, and integrity controls throughout the IoT and AI system lifecycle.

	3.3 Implement advanced cybersecurity techniques (e.g., anomaly detection, secure APIs, adversarial AI defences, device authentication) to safeguard emerging technologies against evolving threats. 3.4 Evaluate the effectiveness of applied security measures through simulation, penetration testing, and compliance assessments with relevant standards (e.g., ISO/IEC 27001, NIST AI RMF).
4. Implement cybersecurity risk management and governance programs based on established standards like NIST and ISO to ensure regulatory compliance and align with business objectives.	4.1 Conduct comprehensive risk assessments using NIST, ISO, and other relevant frameworks to identify threats, vulnerabilities, and business impacts. 4.2 Develop and implement governance, risk, and compliance (GRC) programs that integrate cybersecurity into organisational policies, processes, and strategic objectives. 4.3 Monitor and evaluate the effectiveness of risk management controls through audits, compliance checks, and performance metrics to ensure alignment with regulatory standards. 4.4 Provide risk-based recommendations to stakeholders that balance security requirements with organisational goals, resources, and legal obligations

5. Plan, lead, and perform ethical hacking and penetration testing exercises to identify, analyse, and report on security vulnerabilities, leveraging methodologies from certifications like CEH and OSCP	5.1 Develop penetration testing plans and scopes of work in line with organisational policies, legal frameworks, and ethical standards. 5.2 Execute ethical hacking and penetration testing activities using industry-recognised tools, methodologies, and frameworks (e.g., CEH, OSCP, OWASP). 5.3 Analyse and document discovered vulnerabilities by categorising severity, potential impacts, and exploitability within the organizational context. 5.4 Prepare and present professional reports with actionable remediation strategies to technical teams, management, and stakeholders.
6. Utilize threat intelligence frameworks and methodologies to proactively identify and track threat actors, anticipating attacks and informing defensive security strategies.	6.1 Collect and analyze threat intelligence data from diverse sources (open-source intelligence, dark web, commercial feeds, and internal logs) to identify patterns of malicious activity. 6.2 Apply established threat intelligence frameworks (e.g., MITRE ATT&CK, Diamond Model, Cyber Kill Chain) to profile threat actors and anticipate their tactics, techniques, and procedures (TTPs). 6.3 Correlate threat intelligence findings with organisational vulnerabilities to assess

	potential attack vectors and prioritise defensive actions. 6.4 Develop and disseminate actionable intelligence reports that inform proactive defensive strategies and support decision-making by security teams and executives.
7. Integrate automated security practices into the DevSecOps pipeline to create resilient infrastructure and ensure that security is embedded throughout the software development lifecycle.	7.1 Embed security controls into the DevSecOps pipeline (e.g., static/dynamic code analysis, dependency scanning, container hardening) to detect and remediate vulnerabilities early. 7.2 Automate continuous integration and deployment (CI/CD) security processes to ensure consistent enforcement of policies and secure coding practices. 7.3 Implement infrastructure-as-code (IaC) and automated configuration management tools to build resilient, reproducible, and securely configured environments. 7.4 Monitor and validate pipeline security through automated testing, audit trails, and feedback loops to ensure security remains integrated throughout the SDLC.
8. Lead and guide security teams in the execution of ethical hacking, threat intelligence, and security operations, fostering a culture of collaboration and continuous improvement.	8.1 Coordinate and oversee security team activities in ethical hacking, threat intelligence, and operations to ensure objectives are achieved within scope and compliance requirements. 8.2 Provide mentorship and technical guidance to team members, fostering skill

	development and knowledge sharing in security practices. 8.3 Promote collaboration and communication across multidisciplinary teams to enhance effectiveness, reduce silos, and align with organizational goals. 8.4 Evaluate team performance and implement continuous improvement strategies through feedback, lessons learned, and adoption of best practices.
9. Communicate complex security risks, investment rationales, and strategic security roadmaps to executive leadership and other non-technical stakeholders in a clear, business-oriented manner.	9.1 Translate technical security findings into clear, business-focused language that highlights organizational impact, financial implications, and regulatory relevance. 9.2 Develop and present strategic security roadmaps that align with business objectives, risk appetite, and long-term organizational priorities. 9.3 Justify security investments and resource allocations through cost-benefit analysis, risk reduction metrics, and alignment with business continuity needs. 9.4 Engage effectively with executive leadership and stakeholders using professional reports, visualizations, and presentations tailored to diverse audiences

SECTION C	QUALIFICATION STRUCTURE				
COMPONENT	TITLE	Credits Per Relevant NCQF Level			Total Credits
		Level [6]	Level [7]	Level [8]	
FUNDAMENTAL COMPONENT Subjects/ Courses/ Modules/Units	Fundamentals of Cybersecurity	**20**			**20**
	Computer Networks & Internet Architecture	**20**			**20**
	Programming for Enterprise Security (Python/C)	**20**			**20**
	Discrete Mathematics & Data Handling	**20**			**20**
	Operating Systems & Shell Scripting	**20**			**20**

	Professional Communication & Ethics	**20**			**20**
CORE COMPONENT Subjects/Courses/ Modules/Units	Secure Software Development		**20**		**20**
	Applied Cryptography & PKI		**20**		**20**
	Network Security & SIEM		**20**		**20**
	Identity and Access Architecture		**20**		**20**
	Risk Management & Governance		**20**		**20**
	Digital Forensics & Incident Handling		**20**		**20**
	Enterprise Security Architecture (TOGAF/SABSA)		**20**		**20**
	Cloud & Infrastructure Security (AWS/Azure)		**20**		**20**
	Cyber Threat Intelligence		**20**		**20**

	DevSecOps and Automation		**20**		**20**
	Mini Capstone (Cloud Architecture Design)		**10**		**10**
	Advanced Cloud Security Architecture		**20**		**20**
	Ethical Hacking & Penetration Testing (CEH/OSCP)		**20**		**20**
	Project – Enterprise Capstone		**30**		**30**

STRANDS/ SPECIALIZATION	Subjects/ Courses/ Modules/Units	**Credits Per Relevant NCQF Level**			**Total Credits**
		Level [6]	**Level [7]**	**Level [8]**	
1.					
2.					

Electives **Choose 1 module in level 6 (20 credits) and 2 modules in level 7 (60 credits)**	Mobile & IoT Security	**30**			**30**
	Blockchain & Supply Chain Security	**30**			**30**
	OT & ICS Security		**30**		**30**
	Zero Trust Architectures		**30**		**30**
	Secure AI Systems		**30**		**30**
	Cloud Compliance & Governance		**30**		**30**

SUMMARY OF CREDIT DISTRIBUTION FOR EACH COMPONENT PER NCQF LEVEL	
TOTAL CREDITS PER NCQF LEVEL	
NCQF Level	**Credit Value**
Level 6	**140**
Level 7	**340**
TOTAL CREDITS	**480**

Rules of Combination:

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

- Fundamental: All 120 credits mandatory 20 elective credits in (Level 6).
- Core: All 280 credits mandatory and 60 credits in electives in Level 7,
- Electives: Choose one 30-credit elective in (Level 6) and one in (Level 7), totalling 60 credits.

ASSESSMENT ARRANGEMENTS

Assessment will consist of both formative and summative assessments and should be aligned with learning outcomes and sub-outcomes. Assessment will be conducted by registered and accredited assessors by a recognized regulatory body.

1. Formative Assessment

Formative (50%)

2. **Summative Assessment**

Summative (50%):

MODERATION ARRANGEMENTS

There will be provision for internal and external moderation in accordance with the university policies and regulations, internal and external moderations shall be conducted by qualified moderators or by a recognized regulatory body.

RECOGNITION OF PRIOR LEARNING

There is a provision for award of this qualification through RPL in line with institutional and national policies.

CREDIT ACCUMULATION AND TRANSFER

There is a provision for award of this qualification through credit accumulation in line with institutional and national CAT policies.

PROGRESSION PATHWAYS (LEARNING AND EMPLOYMENT)

Horizontal Articulation:

- BSc Computer Science
- BSc Network Security

Vertical Articulation:

Graduates of this qualification will have the following options for postgraduate education:

- MSc Cybersecurity
- PhD Cybersecurity

Employment Pathways:

- Enterprise Security Architect
- SOC Lead,
- Cloud Security Consultant
- Risk Officer
- ICT Governance Specialist
- Technical Auditor
- Cyber Threat Intelligence Analyst
- DevSecOps Engineer (HRDC-aligned, 32% job growth, BLS 2023).

QUALIFICATION AWARD AND CERTIFICATION

1. Minimum standards of achievement for the award of the qualification

   Candidates meeting the prescribed requirements will be awarded the qualification in accordance with the qualification composition rules and applicable policies. To be eligible for the award of the Bachelor of Science in Enterprise Security Architecture, candidates should have passed all course work assignments and the final examination and obtained a minimum of 480 credits.

2. Certification

   A certificate will be issued to learners who are awarded the qualification.

SUMMARY OF REGIONAL AND INTERNATIONAL COMPARABILITY

This qualification compares with the following:

- BSc in Information Technology (Cybersecurity specialization) - University of Johannesburg (South Africa)
- Bachelor of Science in Enterprise Technology Integration Penn State University USA Though not explicitly named Enterprise Security Architecture, this degree provides a solid foundation relevant for designing secure enterprise-level systems and could lead naturally into security architecture roles.
- Bachelor of Science in Cyber Security University of the Thai Chamber of Commerce (UTCC) Thailand with an emphasis on its inclusion of Enterprise Security Architecture (ESA).

The benchmarking exercise revealed that the proposed (Bachelor of Science in Enterprise Security Architecture (BSc ESA) compares favourably against other regional and international qualifications benchmarked with. The titles vary to denote the qualification streams.

1. Title of Qualification, NQF Level & Credit Value / Duration

Similarity: All are undergraduate bachelor's degrees requiring 3–4 years of study.

Difference: BSc in Information Technology (Cybersecurity specialization) - University of Johannesburg (South Africa) has clear NQF mapping (SA system), Penn State uses U.S. credit-based system, Bachelor of Science in Cyber Security University of the Thai Chamber of Commerce uses modular delivery without widely published credit equivalence.

2. Main Exit Outcomes

Similarity: All aim to produce graduates ready for IT and cybersecurity-linked careers.

Difference: BSc in Information Technology (Cybersecurity specialization) - University of Johannesburg (South Africa) is generalist IT with optional cybersecurity, Penn State emphasizes enterprise integration with applied security potential, Bachelor of Science in Cyber Security University of the Thai Chamber of Commerce is specialized cybersecurity with ESA coverage.

3. Domains / Modules / Courses

Similarity: All cover programming, IT infrastructure, and security.

Difference: BSc in Information Technology (Cybersecurity specialization) - University of Johannesburg (South Africa) is broad with limited dedicated security; Penn State emphasizes business–IT integration; Bachelor of Science in Cyber Security University of the Thai Chamber of Commerce emphasizes practical cyber defense and ESA

4. Assessment Strategies & Weightings

Similarity: All use mixed assessment methods.

Difference: Penn State and Bachelor of Science in Cyber Security University of the Thai Chamber of Commerce emphasize experiential learning (internship/project-heavy). UJ is more traditional exam/coursework-based

5. Qualification Rules & Minimum Standards

Similarity: All require successful completion of a mix of general and specialized modules.

Difference: BSc in Information Technology (Cybersecurity specialization) - University of Johannesburg (South Africa) and Penn State publish clear rules; Bachelor of Science in Cyber Security University of the Thai Chamber of Commerce is less transparent but emphasizes continuous performance.

The proposed qualification Bachelor of Science in Enterprise Security Architecture's career pathways are Enterprise Security Architect SOC Lead, Cloud Security Consultant Risk Officer ICT Governance Specialist Technical Auditor Cyber Threat Intelligence Analyst and DevSecOps Engineer while for benched marked qualifications is Software Security Engineer Information Security, Network Administration, Cybersecurity Consulting, e.g., Security Analyst, Pen tester, IT Security Specialist, or Forensics, cyber security engineer ethical hacker security consultant incident responder security architect forensic computer analyst security software developer cryptographer, and cyber security analyst. The educational and career pathways compare favourably, and graduates of the proposed qualification will not be disadvantaged in the job markets

REVIEW PERIOD
The qualification will be reviewed every 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**	