Bachelor of Applied Science in Cyber Operations (with Emphasis in Defense/Forensics) - IC410 (Under Review)

1. Introduction

The University of Mauritius (UoM) and the University of Arizona (UA) have partnered to offer an innovative dual degree programme in Cyber Operations with an emphasis in Defense and Forensics. The Bachelor of Applied Science (BAS) degree in Cyber Operations is an interdisciplinary Cyber education programme. The Defense & Forensics Track conforms to academic requirements from both the US National Security Agency's Centers of Academic Excellence in Cyber Operations (CAE-CO) and US Cyber Defense (CAE-CD). The University of Arizona's BAS in Cyber Operations has earned a Silver Seal from the Service members Opportunity Colleges (SOC) organization as part of their Cybersecurity Network. SOC is a US Department of Defense initiative designed to identify trusted, high-quality educational credentials that accommodate the specific needs of active duty Service members.
The BAS in Cyber Operations prepares students for entry into a number of cyber-related occupations in defense, law enforcement, and private industry. The curriculum includes both offensive and defensive cyber security content delivered within the state-of-the-art Cyber Virtual Learning Environment (VLE) to ensure that students have extensive hands-on experience to develop the knowledge, skills, and abilities necessary to succeed after they graduate. Through this partnership students can complete two degrees in cyber operations without having to leave Mauritius. Upon completion, students may graduate with degrees from both the University of Mauritius and the University of Arizona.

Career Opportunities
According to the U.S. Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 37% from 2012 to 2022. A rate which is much faster than the average for all other occupations and it is expected that there will be a global shortage of 6 million cyber security professionals by 2019.

2. Objectives

This programme has been designed to enable students to:

- gain the hands-on knowledge, skills, and abilities necessary to excel in the Cyber field. This programme delivers highly technical Cyber content through its world class Virtual Learning Environment.
- maximize the opportunity for students to gain the hands-on experience to become successful cyber professionals.
- to learn the concepts and technologies and to demonstrate that they have mastered the course content through hands-on exercises and interactive assessments.
- analyze all technical security, legal and financial issues in real-world cases.
- recognize appropriate techniques to minimize risks.
- develop the ability to provide swift response to security breaches and threats.
- investigate techniques and tools specific to network, system software, and application software security.
- study ways to structure computer-security practices in alignment with organizational needs.
- have a deep understanding of the psychological aspects of cyber operations

3. General Entry Requirements

As per the General Entry Requirements for Admission to the University for Undergraduate Degrees.

4. Programme Entry Requirements

At least 2 GCE 'A' Level Passes including Mathematics or any other qualification acceptable to the University of Mauritius.

International students will have to satisfy the UA admission merit criteria. Click on the link below: https://admissions.arizona.edu/how-to-apply/international/country-requirements .

5. Minimum Requirements for Awards

(i) Degree (Awarded by both UoM and UA)
For the degree award in BAS in Cyber Operations, the student must obtain at least 120 credits including:

Modules	**Credits**
Minimum Credits for UoM ICT modules	44
Minimum Credits for UoM GenEd modules	27
Minimum Credits for UA modules	49
TOTAL	**120**

(ii) Diploma Award (Awarded by UoM only)

The Diploma is provided as a possible exit point in the programme. A student may opt for a Diploma in Information and Communication Technologies by making a written request to the Dean or in case of termination. Award of Diploma will be granted provided he/she has obtained a minimum of 80 credits.

(iii) Certificate Award (Awarded by UoM only)

The Certificate is provided as a possible exit point in the programme. A student may opt for a Certificate in Information and Communication Technologies by making a written request to the Dean or in case of termination. Award of Certificate will be granted provided he/she has obtained a minimum of 40 credits.

6. Programme Duration

	Normal (Years)	**Maximum (Years)**
Degree:	4	7

7. Credits per Semester

Students may register for a minimum of 12 credits and a maximum of 19 credits per semester.

8. Classification of Awards for the Programme

The award classification will be based on the grade point system in place at the University of Arizona.

This honor, based upon graduation grade-point-average, becomes part of the official record, is awarded upon graduation and appears on the transcript and diploma of the recipient.

1. Summa Cum Laude -- is awarded to candidates whose grade-point-average is 3.900 or higher.
2. Magna Cum Laude -- is awarded to candidates whose grade-point-average is 3.700-3.899.
3. Cum Laude -- is awarded to candidates whose grade-point-average is 3.5000-3.699.
4. Graduate -- is awarded to candidates whose grade-point-average is 2.000-3.499.

The grading system in place at Arizona University is as follows.

GRADING SCALE		DISTRIBUTION	
A	90 to 100%	900 – 1000 Points	A
B	80 to 89%	800 – 899 Points	B
C	70 to 79%	700 – 799 Points	C
D	60 to 69%	600 – 699 Points	D
E	Below 60%	0 – 599 Points	E

Grade	Point
A	4
B	3
C	2
D	1
E	0

9. Academic Progress as per University of Arizona policy

Undergraduate students will be considered to be making normal progress toward a degree if their cumulative grade-point-average (GPA) for all work attempted at the University of Arizona is not less than 2.000.

One of the requirements for undergraduates to be eligible to continue at the University is that they earn a minimum cumulative grade-point-average (GPA) of 2.000.

Undergraduate students not meeting academic progress will be placed on academic probation. Academic probation status occurs following any semester when the student's cumulative grade-point-average (GPA) drops below a 2.000. The first time that students are placed on academic probation, they should meet with their academic advisor (link is external) to discuss the consequences, such as enrollment in a mandatory Academic Recovery Program during the following semester 1 or 2. Students on academic probation are subject to restrictions or requirements, such as certain courses/module that are determined by the faculty in which the student is enrolled. Students are removed from academic probation upon earning the minimum 2.000 cumulative GPA as required by the University. However, if student's GPA drops below 2.00 after coming out of probation, the student may be terminated from the programme of study.

10. Pre-Requisite Modules (PR)

A student will be allowed to follow module *y* of which module *x* is a pre-requisite (PR) provided he/she has **satisfactorily completed module *x* with at least a pass grade**.

11. Assessment and Pass Requirements

The assessment mode for each module will be based on one or a combination of the following:

- Examination
- Continuous Assessment (class tests, assignments, practicals and oral presentations)
- Report Assessment
- Software Evaluation

An overall total of at least 60% for combined continuous assessment and written examination components would be required to pass the module. The specific details and/or formula for the calculation of the final mark are given in the MSS (Module Specification Sheet) for each module. Students have to retake both continuous assessments and exams in modules in which they have failed.

12. Programme Plan

Year 1, Semester 1

Module Code	Module	UoM Credits	UA Unit Conversion
ENG110	English Composition I	3	3
ICT110	Mathematics for IT	4	4
ICT111	Fundamentals of Computer Science	3	3
Elective Code *	Any one Foreign Language from available list as per 13(iii)(a) or *	3	3
SAS101	Student Success Course	1	1
ICT112	The Digital World	3	3
	Semester Total	**17**	**17**

** Or an alternate elective as approved by the Faculty.*

Year 1, Semester 2

Module Code	Module	UoM Credits	UA Unit Conversion
ENG111	English Composition II	3	3
ICT121	Basic Operating Systems	3	3
ICT122	Introduction to Computer Programming	3	3
ICT123	Database Basics	3	3
BASV 314	Mathematics for Applied Sciences	3	3
	Semester Total	**15**	**15**

Year 2, Semester 1

Module Code	Module	UoM Credits	UA Unit Conversion
ICT210	Scripting for the Web	4	4
ICT211	Networking Principles I	3	3
ICT212	System Administration I	3	3
CYBV 301	Fundamentals of Cybersecurity	3	3
ENGV 306 ***OR*** ENGV 308	Advanced Composition ***OR*** Technical Writing	3 3	3 3
	Semester Total	**16**	**16**

Year 2, Semester 2

Module Code	Module	UoM Credits	UA Unit Conversion
ICT222	System Administration II	3	3
ICT221	Networking Principles II	3	3
INFV 320	Computational Thinking & Doing	3	3
CYBV 385	Introduction to Cyber Operations	3	3
HIST2223 ***OR*** POLI220	Contemporary Mauritius – Institutions , Diversity and Society ***OR*** Democracy and Democratisation	3 3	3 3
	Semester Total	**15**	**15**

Year 3, Semester 1

Module Code	Module	UoM Credits	UA Unit Conversion
BASV 326	Introductory Methods of Network Analysis	3	3
CYBV 388	Cyber Investigations & Forensics	3	3
CYBV 400	Active Cyber Defense	3	3
DGT311	Digital Multimedia Concepts	3	3
ICT310	Bioinformatics	3	3
	Semester Total	**15**	**15**

Year 3, Semester 2

Module Code	Module	UoM Credits	UA Unit Conversion
CYBV 480	Cyber Warfare	3	3
CYBV 477	Advanced Cyber Forensics	3	3
ICT325	Mobile and Wireless Technologies	3	3
COMS3205	Critical Media Literacies	3	3
COMS3206	Digital Media Cultures	3	3
	Semester Total	**15**	**15**

Year 4, Semester 1

Module Code	Module	UoM Credits	UA Unit Conversion
ICT410	Secure Coding	3	3
SOCI410	Sustainable Development Practices	3	3
BASV 329	Cyber Law, Ethics & Policy	3	3
CYBV 479	Wireless Networking and Security	3	3
CYBV 379	Cloud Computing	3	3
	Semester Total	**15**	**15**

Year 4 -Semester 2

Module Code	Module	UoM Credits	UA Unit Conversion
CYBV 435	Cyber Threat Intelligence	3	3
CYBV 454	Malware Threats & Analysis	3	3
CYBV 498	Cyber Operations Senior Capstone	3	3
PSY420	Forensic Psychology	3	3
	Semester Total	**12**	**12**
	Degree Total	**120**	**120**

Note:

1. *The University reserves the right not to offer a given elective module if the critical number of students is not attained and/or for reasons of resource constraints.*

13. (i) List of CORE Modules from UoM

ENG110: English Composition I (L-3)
ICT110: Mathematics for IT (L-4)
ICT111: Fundamentals of Computer Science (L/P: 2+2)
ICT112: The Digital World (L-3)
ENG111: English Composition II (L-3)
ICT121: Basic Operating Systems (L/P: 2+2)
ICT122: Introduction to Computer Programming (L/P: 2+2)
ICT123: Database Basics (L/P: 2+2)
ICT210: Scripting for the Web (L/P: 2+4)
ICT211: Networking Principles I (L/P: 2+2)
ICT212: System Administration I (L/P: 2+2)
ICT222: System Administration II (L/P: 2+2)
ICT221: Networking Principles II (L/P: 2+2)
DGT311: Digital Multimedia Concepts (L/P: 3+0)
ICT310: Bioinformatics (L/P: 2+2)
ICT325: Mobile and Wireless Technologies (L-3)
COMS3205: Critical Media Literacies (L-3)
COMS3206: Digital Media Cultures (L-3)
ICT410: Secure Coding (L/P: 2+2)
SOCI410: Sustainable Development Practices (L-3)
PSY420: Forensic Psychology (L-3)

(ii) List of CORE Modules from UA
SAS 101: Student Success Course (L-1)
BASV 314: Mathematics for Applied Sciences (L-3)
CYBV 301: Fundamentals of Cybersecurity (L/P: 2+2)
INFV 320: Computational Thinking & Doing (L/P: 2+2)
CYBV 385: Introduction to Cyber Operations (L/P: 2+2)
BASV 326: Introductory Methods of Network Analysis (L/P: 2+2)
CYBV 388: Cyber Investigations & Forensics (L/P: 2+2)
CYBV 400: Active Cyber Defense (L/P: 2+2)
CYBV 480: Cyber Warfare (L/P: 2+2)
CYBV 477: Advanced Cyber Forensics (L/P: 2+2)
BASV 329: Cyber Law, Ethics & Policy (L-3)
CYBV 479: Wireless Networking and Security (L-3)
CYBV 379: Cloud Computing (L/P: 2+2)
CYBV 435: Cyber Threat Intelligence (L/P: 2+2)
CYBV 454: Malware Threats & Analysis (L/P: 2+2)
CYBV 498: Cyber Operations Senior Capstone

(iii)List of Electives from UoM **

(a) Foreign Language Modules
HUM110: Chinese/ (L-3)
HUM111: German (L-3)
FREN1122: French for Beginners (L-3)

(b) History and Political Modules
HIST2223: Contemporary Mauritius – Institutions, Diversity and Society (L-3)
POLI220: Democracy and Democratisation (L-3)

******* *The University reserves the right to review the list of electives.*

(iv) List of Electives from UA
ENGV 306: Advanced Composition (L-3)
ENGV 308: Technical Writing (L-3)