

ACU Dallas Approval Chart for Curriculum Changes

A = Approve I = Information Item R = Advise & Respond

Course Number: **or Degree Plan(s): BS Cybersecurity**

Program title: Bachelor of Science in Cybersecurity

Degree type: Bachelor of Science

The Bachelor of Science in Cybersecurity program is a flexible major that prepares students in various areas of computing such as programming, database management, web development, and computer networking. The primary focus is on securing an organization's digital infrastructure. Hardening devices, testing systems for vulnerabilities, assessing risk, and developing policies are all part of the program curriculum.

The Degree in Cybersecurity will utilize all of the courses in the BSITA Information Assurance concentration and will add the following five (5) new courses:

ITA 121 PC Service and Support 1

ITA 122 PC Service and Support 2

ITA 332 Cloud and Network Defense

ITA 336 System Forensics

ITA 445 System Vulnerability Testing

Highlight the item that corresponds to the requested change.

	Change to a Course	o	a	A	O	S
1.	Title (description unchanged)	A	A	I	I	I
2.	Description (not affecting content)	A	A	I	I	I
3.	Course term(s)	A	A	I	I	I
4.	Content (substantive change)	A	A	A	A	I
5.	Number of credit hours	A	A	A	A	I
6.	Course number within the hundred	A	A	I	I	I
7.	Course number beyond the hundred	A	A	A	A	I
8.	Prerequisites	A	A	A	A	I
9.	Course fee(s)	A	A	--	A	I
10.	From U to G or G to U	A	A	A	A	I
11.	Cross list with another program or department	A	A	A	A	I
12.	Program/department of record	A	A	A	A	I
13.	Open or close a course	A	A	A	A	I

14.	New course (application required)	A	A	A	A	I
-----	-----------------------------------	---	---	---	---	---

	Change to a Degree Plan	Program	College	Academic	Office	Student	Faculty
1.	Major/Program — Revision	A	A	A	A	A	--
2.	Major/Program — Adopt or change admission requirements	A	A	A	A	A	--
3.	Major/Program — Add	A	A	A	A	A	--
4.	Major/Program — Offer existing university program on campus	--	A	A	A	A	--
5.	Major/Program — Discontinue (proposed by Program or College)	A	A	A	A	A	I
6.	Major/Program — Discontinue (proposed by Provost)	R	R	A	A	A	I
7.	GPA — Revise major/program or cumulative requirement	A	A	A	A	A	--
8.	Minor — Revise course selection	A	A	I	I	I	--
9.	Minor — Add	A	A	A	A	A	--
10.	Minor — Discontinue (proposed by Program or College)	A	A	A	A	A	--
11.	Minor — Discontinue (proposed by Provost)	R	R	A	A	A	--
12.	Degree — Add	A	A	A	A	A	I
13.	Degree — Discontinue (proposed by Program or College)	A	A	A	A	A	I
14.	Degree — Discontinue (proposed by Provost)	R	R	A	A	A	I

	Change to Undergraduate University Requirements	A	A	A	A	A	A	A	A
15.	University Requirements — Change in approved course content	A	A	A	A	A	A	--	A
16.	University Requirements — Add or drop a required course from the University Requirements chart	A	A	A	A	A	A	A	A
17.	University Requirements — Add or drop a course from a menu within the University Requirements chart	A	--	--	A	A	A	--	A
18.	University Requirements — Change hours within a menu on the University Requirements chart	A	A	A	A	A	A	A	A
	Change to Catalog Information For Campus								
1.	General requirements for graduation including course requirements that are common to all majors for all degrees	--	--	A	--	--	A	--	A
2.	Admission requirements	--	--	A	--	--	A	--	A
3.	Policies governing academic probation and suspension	--	--	A	--	--	A	--	A
4.	Requirements for graduating with honors	--	--	A	--	--	A	--	A

Dr. Joe Feliciano

Program Director/Department Chair

May 12, 2023

Signature

Date

Signature

Date

Dean(s)

Marlene W. G., Ph.D.

May 12, 2023

Signature

Date

Signature

Date

College Academic Council

Chair's Signature

Date

Chair's signature

Date

University General Education Council

Chair's signature

Date

Undergraduate Academic Council

Chair's signature

Date

Provost

Signature

Date

Faculty

Faculty Senate Chair's signature

Date

President

Signature

Date

Bachelor of Science in Cybersecurity New Program Application

1. Program Identification

- a. Program title: **Bachelor of Science in Cybersecurity**
- b. Degree type: Bachelor of Science
- c. Home department or unit: School of Professional Studies, College of Graduate and Professional Studies
- d. Program developer(s) and credentials: Dr. Joe Feliciano
- e. Where program will be offered and delivery method: ACU Dallas, Online
- f. Proposed date of implementation: Fall 1
- g. CIP: 11.1003 - Computer and Information Systems Security
- h. Formstack:
 - i. Program Code: BS CYBR
 - ii. Major Code: CYBER
 - iii. Concentration Code:
 - iv. Degree Type: Baccalaureate
 - v. Program Category:
 - vi. Minimum Education Required: High School
 - vii. Credit Hours: 120
 - viii. Program Length (Months):
 - ix. Number of Tracks: 0
 - x. Track Names:

2. Program Details

- a. Program description.

The Bachelor of Science in Cybersecurity program is a flexible major that prepares students in various areas of computing such as programming, database management, web development, and computer networking. The primary focus is on securing an organization's digital infrastructure. Hardening devices, testing systems for vulnerabilities, assessing risk, and developing policies are all part of the program curriculum.
- b. Program mission statement.

The mission of the Bachelor of Science in Cybersecurity is to equip students to secure digital infrastructures with a set of professional skills that provides opportunities to offer Christian service and leadership in their careers and communities.
- c. Program outcomes.

The Program Outcomes (POs) for the Bachelor of Science in Cybersecurity are as follows. All students will meet Outcomes 1-6.

PO #1. Programming

Students will be able to code at a level appropriate to develop software solutions for use in security assessments, system integration, maintenance, or optimization.

PO #2 Managing Data

Students will be able to apply current tools and techniques to manage organizational data.

PO #3 Networks and Communication Infrastructure

Students will be able to apply current tools and techniques to manage an organization's network and communications infrastructure.

PO #4. System Defense, Testing, and Breach Investigation

Students will be able to apply current tools and techniques to secure an organization's information and communications infrastructure.

PO #5. Computer hardware, Operating Systems, and User technological Support

Students will be able to apply current tools and techniques to support client/server software and hardware systems.

PO #6: IT Professional Skills, Ethical and Social Responsibility

Students will be able to identify and apply ethical principles to complete tasks required by IT professionals, such as but not limited to managing projects and communicating with users.

d. Description of target audience.

The Bachelor of Science in Cybersecurity is intended for working students seeking a bachelor's degree online. The degree is specifically designed for students who are seeking to expand their career opportunities in technology and systems security by gaining a bachelor's degree in information technology with a security focus.

e. Admission requirements.

- i. Application and processing fee.
- ii. Abilene Christian University's Online Baccalaureate programs are intended for non-traditional students interested in obtaining a bachelor's degree online. Students who have earned a GED must be at least 22 years of age. Exceptions to these requirements may be made for transfer students matriculating from an institution with an articulation agreement with ACU.
- iii. Purpose statement addressing career goals.

- iv. Resume or CV.
 - v. There are no prerequisites for this program
 - vi. International applicants will be required to provide TOEFL scores (if applicable) and transcript assessment for degrees completed outside of the United States.
- f. Projected total enrollment for each of the first five years.
 - i. Year 1: 25
 - ii. Year 2: 50
 - iii. Year 3: 75
 - iv. Year 4: 100
 - v. Year 5: 115
- g. CIP code. 11.1003

3. Rationale and Need for Program

- i. Mission fit.

CGPS already provides academic programs for Information Technology at the undergraduate and graduate levels and a certificate in Cybersecurity at the graduate level. This innovative program addresses the needs of an emerging market in cybersecurity and offers students the opportunity to serve businesses and communities from personal devices to critical infrastructure; a demand which couples knowledge and skill in technology with ethics and integrity in character. In short, this prepares students for Christian service in a vital and growing need.
- j. Societal need.

Cybersecurity personnel play a crucial role in protecting our society from cyber threats. With the increasing reliance on technology in all aspects of our lives, from personal devices to critical infrastructure, the need for individuals with the skills to secure these systems has never been greater. Cybersecurity personnel work to detect and prevent cyber attacks on networks and systems and also to develop strategies and plans to mitigate the effects of those attacks when they do occur. They help to ensure the confidentiality, integrity, and availability of sensitive information and play a key role in protecting individuals and organizations from financial loss, reputational damage, and other harm. Additionally, as the nature of cyber threats is constantly evolving, cybersecurity personnel must continuously update their knowledge and skills to stay ahead of the latest threats and to protect against them effectively.

- k. Employment demand and career possibilities.
- i. Identify jobs that graduates would be qualified to pursue.: Occupations include the following titles... ¹
 - Information security analyst
 - Software security engineer
 - Security architect
 - Penetration tester
 - Chief information security officer
 - Information security crime investigator
 - Security consultant
 - ii. Employment demand in the State of Texas:
 - There are currently 289,480 jobs in the state that map to this CIP code (using Lightcast mapping heuristic). There has been a growth of 15.6% over the past three years in Texas, compared to national growth of 8.3% in this field.
 - There are currently 41,081 positions open annually. There were 629,011 jobs posted over the past 12 months, with a posting intensity of 3:1 (average).
 - Median income for this field in Texas is \$95.2K/year
- l. Prospective student interest.
- There are currently 27 programs with this CIP in the State of Texas, with 1,344 completions in 2021 (most recent data available from IPEDS). This represents a 178% growth for the last five years in this program. Only 13 institutions in Texas offer this program in distance format, and those programs have enjoyed a growth of 442% over the past five years.
- m. Disciplinary benchmarking.
- The program proposed in this proposal is consistent with other programs in the State. An eventual plan to offer undergraduate certificates will represent a significant opportunity to add “Direct to Business” opportunities to this program as well.

4. Curriculum

- a. Degree plan
- University Requirements (54 hours)**
- MATO 131 (Credit Hours: 3)*
- or
- MATH 185 (Credit Hours: 3)*

¹ Indeed Editorial Team (2022, Apr 14). What does a cybersecurity specialist do? A definitive guide. Indeed Career Guide. Retrieved from <https://www.indeed.com/career-advice/finding-a-job/what-does-cyber-security-specialist-do>

Programming (6 Hours)

CSO 115 (Credit Hours: 3)

CSO 116 (Credit Hours: 3)

Information Technology (27 Hours)

ITA 110 (Credit Hours: 3)

ITO 220 (Credit Hours: 3)

ITO 221 (Credit Hours: 3)

ITO 320 (Credit Hours: 3)

ITO 410 (Credit Hours: 3)

ITC 460 (Credit Hours: 3)

ITA 491 (Credit Hours: 3)

ITA 121 (Credit Hours: 3)

ITA 122 (Credit Hours: 3)

Mathematics (3 Hours)

MATO 131 (Credit Hours: 3)*

or

MATH 185 (Credit Hours: 3)*

MATO 377

**May be used to satisfy University Requirements.*

Cybersecurity (21 Hours)

ITO 310 (Credit Hours: 3)

ITA 332 (Credit Hours: 3)

ITA 336 (Credit Hours: 3)

ITA 445 (Credit Hours: 3)

ITO 415 (Credit Hours: 3)

ITO 473 (Credit Hours: 3)

ITA 475 (Credit Hours: 3)

Total: 57 Credit Hours

Electives

9 Credit Hours

Total Major Hours: 66

Other Graduation Requirements

Minimum GPA in major: 2.00

Minimum GPA for graduation: 2.00

Minimum advanced hours: 33

Minimum total hours: 120

*Courses numbered 0** do not count in minimum hours required for degree.*

b. Courses.

Course	Req'd or Menu	Aligned POs (i) = Introduced (r) = Reinforced (m) = Mastered	Rotation and Frequency	Faculty Credentialed to Teach
ITA 110 - Introduction to Information, Technology, and Computing	Req'd	PO#6 (i)	Every second part of term (fall2, spring 2, summer 2)	MS in CS, IT or related field
CSO 115 - Introduction to Programming Using Scripting	Req'd	PO #1 (i)	Every first part of term (fall 1, spring 1, summer 1)	MS in CS, IT or related field
CSO 116 - Applied Programming Using Scripting	Req'd	PO #1 (m)	Every second part of term (fall2, spring 2, summer 2)	MS in CS, IT or related field
ITO 220 - Introduction to Databases and Database	Req'd	PO #2 (i)	Every second part of term (fall2, spring 2, summer 2)	MS in CS, IT or related field

Management Systems				
ITO 221 - Fundamentals of Networking and Data Communications	Req'd	PO #3 (i)	Every second part of term (fall2, spring 2, summer 2)	MS in CS, IT or related field
ITO 310 - Introduction to Computer and Information Security	Req'd	PO#4 (i)	Every second part of term (fall2, spring 2, summer 2)	MS in CS, IT or related field
ITO 320 - Database Administration	Req'd	PO#2 (m)	Every first part of term (fall 1, spring 1, summer 1)	MS in CS, IT or related field
ITO 410 - Systems Integration and Administration	Req'd	PO#5 (r)	Every first part of term (fall 1, spring 1, summer 1)	MS in CS, IT or related field
ITA 491 - Emerging Technologies in IT (Writing Intensive and Capstone)	Req'd	PO#6 (m)	Every second part of term (fall2, spring 2, summer 2)	MS in CS, IT or related field
ITA 460 - Managing Technical Projects		PO#6 (m)	Every first part of term (fall 1, spring 1, summer 1)	MS in CS, IT or related field

MATH 377 - Statistical Methods I	Required			
MATH 131 - Calculus for Application	Required			
ITO 415 - Networks and Security	Req'd	PO#3 (r)	Run every three terms.(Spring 1 and Summer 2)	MS in CS, IT or related field
ITO 473 - Cybersecurity Policies, Standards, and Compliance	Req'd	PO#4 (r)	Run every three terms.(Spring 2 and Fall 1)	MS in Cybersecurity, Information Assurance, or related field
ITA 475 - Risk and Incident Planning and Response	Req'd	PO#4 (m)	Run every three terms.(Summer 1 and Fall 2)	MS in Cybersecurity, Information Assurance, or related field
ITA 121 PC Service and Support 1	Req'd	PO#5 (i)	Add to course planning calendar	MS in CS, IT or related field
ITA 122 PC Service and Support 2	Req'd	PO#5 (m)	Add to course planning calendar	MS in CS, IT or related field
ITA 332 Cloud and Network Defense	Req'd	PO#4 (m)	Add to course planning calendar	MS in Cybersecurity, Information Assurance, or related field
ITA 336 System Forensics	Req'd	PO#4 (m)	Add to course planning calendar	MS in Cybersecurity, Information Assurance, or related field

ITA 445 System vulnerability Testing	Req'd	PO#4 (m)	Add to course planning calendar	MS in Cybersecurity, Information Assurance, or related field
---	-------	----------	---------------------------------	---

c. New courses.

i. Courses

- ITA 121 PC Service and Support 1

This course concentrates on the fundamentals of computer hardware. Students will be able to describe the internal components of a computer, assemble a computer system, and troubleshoot using system tools and diagnostic software. Students will also learn to connect to the Internet and share resources in a network environment.

- ITA 122 PC Service and Support 2

Provides an in-depth look at advanced computer maintenance concepts and techniques. Topics include PC development techniques, troubleshooting strategies, advancement of technological development and problem-solving strategies.

- ITA 332 Cloud and Network Defense

In this course students will apply tools and methods to secure organizational data and communication infrastructures. Challenges in providing security and effective defense for cloud, mobile, and remote systems are discussed.

- ITA 336 System Forensics

This course is designed to present methods for assessing potential breaches and determining the scope and possible impacts. Methods such as log analysis, file metadata review, chain of custody, and legal processes are presented.

- ITA 445 System Vulnerability Testing

This is a hands-on course that provides skills in assessing system vulnerabilities. Processes, tools, and methods for penetration testing are explored.

- ii. Curriculum approval schedule will be negotiated with the provost's office during initial review.

The program director has indicated that applications for the five new courses listed below will come forward with the new program proposal. If any of the course proposals needs to be delayed, it should be submitted to the CGPS Academic Council no later than February 2024. The program's degree audit will not function correctly until all courses are approved and added to the catalog.

- ITA 121 PC Service and Support 1
- ITA 122 PC Service and Support 2
- ITA 332 Cloud and Network Defense
- ITA 336 System Forensics
- ITA 445 System vulnerabilities and Penetration Systems

5. Assessment Plan

- a. Curriculum map: See table above. (i) are courses where an outcome is introduced. (r) are courses where outcomes are reinforced, and (m) are courses where students will master the outcome.
- b. Outcome assessment measures.

PO #1. Programming

Program Outcome #1 Measure #1

PO#1 Students will be able to code at a level appropriate to develop software solutions for use in security assessments, system integration, maintenance, or optimization.

Details/Description:

CSO116 Applied Programming Using Scripting

W5 Assignment 1: Programming Assignment 3: Lists & Dictionaries

In this assignment students develop algorithms to solve problems encountered while programming. They also write programs that use files for input/output.

Level of Proficiency Target (Competency Target):

80 % of students will attain a raw score (before any penalties) of 80% or better on this programming exercise.

Ideal Target:

80 % of students will attain a raw score (before any penalties) of 90% or better

Implementation Plan (timeline):

This objective will be measured annually.

Key/Responsible Personnel:
ALL BSITA Faculty

PO #1. Programming
Program Outcome #1 Measure #2

PO#1 Students will be able to code at a level appropriate to develop software solutions for use in security assessments, system integration, maintenance, or optimization.

Details/Description:
CSO 115 Introduction to Programming Using Scripting
W7 Assignment 2: Pass by Value
Create a function that will receive a numeric parameter variable. This function will print your name X number of times based on the value of the parameter.

Level of Proficiency Target (Competency Target):
80 % of students will attain a raw score (before any penalties) of 80% or better on this programming exercise.

Ideal Target:
80 % of students will attain a raw score (before any penalties) of 90% or better on this programming exercise.

Implementation Plan (timeline):
This objective will be measured annually.

Key/Responsible Personnel:
ALL BSITA Faculty

PO #2 Managing Data
Program Outcome #2 Measure #1

PO#2 Students will be able to apply current tools and techniques to manage organizational data.

Details/Description:
ITO 320: Database Administration
W6 Assignment 2: Managing Data Security in a DBMS
Practical exercise in planning and implementing the principles and practices for establishing and managing data security in a database using a DBMS.

Level of Proficiency Target (Competency Target):
Goal - 80% of students will attain an 80% or greater

Ideal Target:

Ideal - 90% of students will attain a 90% or greater

Implementation Plan (timeline):

This objective will be measured annually

Key/Responsible Personnel:

ALL BSITA Faculty

PO #2 Managing Data

Program Outcome #2 Measure #2

PO#2 Students will be able to apply current tools and techniques to manage organizational data.

Details/Description:

ITO 320: Database Administration

W2 Assignment 1: DBMS Installation

Practical experience in preparing for a DBMS installation, the installation process(s), and the configuration. This exercise also practices the importance of documentation in a data environment.

Level of Proficiency Target (Competency Target):

Goal - 80% of students will attain an 80% or greater

Ideal Target:

Ideal - 90% of students will attain a 90% or greater

Implementation Plan (timeline):

This objective will be measured annually

Key/Responsible Personnel:

ALL BSITA Faculty

PO #3 Networks and Communication Infrastructure

Program Outcome #3 Measure #1

PO#3 Students will be able to apply current tools and techniques to manage an organization's network and communications infrastructure.

Details/Description

ITO 221 - Fundamentals of Network & Data Communication:

W1 Discussion Question 2: Using the OSI model for network problems
Students will learn how to use the OSI model to isolate a network problem.

Level of Proficiency Target (Competency Target):
Goal - 80% of students will attain an 80% or greater

Ideal Target:
Ideal - 90% of students will attain a 90% or greater

Implementation Plan (timeline):
This objective will be measured annually

Key/Responsible Personnel:
ALL BSITA Faculty

PO #3 Networks and Communication Infrastructure
Program Outcome #3 Measure #2

PO#3 Students will be able to apply current tools and techniques to manage an organization's network and communications infrastructure.

Details/Description
ITO 221 - Fundamentals of Network & Data Communication:
W6 Assignment 3: Term Project - Computer Networking Slideshow Presentation
The purpose of this term project is to research a networking concept or technology and present it in a visually stimulating way to a specific audience.

Level of Proficiency Target (Competency Target):
Goal - 80% of students will attain an 80% or greater

Ideal Target:
Ideal - 90% of students will attain a 90% or greater

Implementation Plan (timeline):
This objective will be measured annually

Key/Responsible Personnel:
ALL BSITA Faculty

PO #4. System Defense, Testing, and Breach Investigation
Program Outcome #4 Measure #1

PO#4 Students will be able to apply current tools and techniques to secure an organization's information and communications infrastructure.

Details/Description:

ITO 415 Networks and Security Administration

W6 Assignment 1: Keeping Your Head Securely in the Cloud

By engaging in discussion, students will start to learn and understand apply security standards in an organization

Level of Proficiency Target (Competency Target):

Goal - 80% of students will attain an 80% or greater

Ideal Target:

Ideal - 90% of students will attain a 90% or greater

Implementation Plan (timeline):

This objective will be measured annually

Key/Responsible Personnel:

ALL BSITA Faculty

PO #4. System Defense, Testing, and Breach Investigation

Program Outcome #4 Measure #2

PO#4 Students will be able to apply current tools and techniques to secure an organization's information and communications infrastructure.

Details/Description:

ITO 310: Intro to Computer and Information Security

W5 Assignment 1: Analyzing Encryption Techniques

The purpose of this assignment is to explore the various types of encryption and their application.

Level of Proficiency Target (Competency Target):

Goal - 80% of students will attain an 80% or greater

Ideal Target:

Ideal - 90% of students will attain a 90% or greater

Implementation Plan (timeline):

This objective will be measured annually

Key/Responsible Personnel:

ALL BSITA Faculty

PO #5. Computer hardware, Operating Systems, and User technological Support

Program Outcome #5 Measure #1

PO#5 Students will be able to apply current tools and techniques to support client/server software and hardware systems.

Details/Description:

ITO 410: Systems Integration and Administration

W2 Discussion Question 1: Windows PowerShell - Device Drivers

Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration. Students learn how the use of this tool can greatly expedite admin tasks.

Level of Proficiency Target (Competency Target):

80 % of students will attain a raw score (before any penalties) of 80% or better.

Ideal Target:

90 % of students will attain a raw score (before any penalties) of 90% or better.

Implementation Plan (timeline):

This objective will be measured annually

Key/Responsible Personnel: ALL BSITA Faculty

PO #5. Computer hardware, Operating Systems, and User technological Support

Program Outcome #5 Measure #2

PO#5 Students will be able to apply current tools and techniques to support client/server software and hardware systems.

Details/Description:

ITO 410: Systems Integration and Administration

W3 Assignment 2 (Part 2): Lab 5-1: Configuring Advanced Storage Solutions

Students configure Network File Systems (NFS) data store and configure Central Access Rules and Policies.

Level of Proficiency Target (Competency Target):

80 % of students will attain a raw score (before any penalties) of 80% or better.

Ideal Target:

90 % of students will attain a raw score (before any penalties) of 90% or better.

Implementation Plan (timeline):

This objective will be measured annually

Key/Responsible Personnel: ALL BSITA Faculty

PO #6: IT Professional Skills, Ethical and Social Responsibility

Program Outcome #6 Measure #1

PO#6 Students will be able to identify and apply ethical principles to complete tasks required by IT professionals, such as but not limited to managing projects and communicating with users.

Details/Description:

ITA 445 System vulnerability Testing

W1 Assignment 1: Ethics for Pen Testing

In this assignment students will outline the ethical implications surrounding a network vulnerability test and the items required before work can begin.

Level of Proficiency Target (Competency Target):

80 % of students will attain a raw score (before any penalties) of 80% or better.

Ideal Target:

80 % of students will attain a raw score (before any penalties) of 90% or better.

Implementation Plan (timeline):

This objective will be measured annually.

Key/Responsible Personnel:

ALL BSITA Faculty

PO #6: IT Professional Skills, Ethical and Social Responsibility

Program Outcome #6 Measure #2

PO#6 Students will be able to identify and apply ethical principles to complete tasks required by IT professionals, such as but not limited to managing projects and communicating with users.

Details/Description:

ITA 491 Emerging Technologies in IT

W2 Assignment 1: Challenges to Adopting Emerging Technologies

The purpose of this assignment is to address the challenges of adopting emerging technologies.

Level of Proficiency Target (Competency Target):

80 % of students will attain a raw score (before any penalties) of 80% or better.

Ideal Target:

80 % of students will attain a raw score (before any penalties) of 90% or better.

Implementation Plan (timeline):

This objective will be measured annually.

Key/Responsible Personnel:

ALL BSITA Faculty

- c. Description of assessment cycle:
 - i. PO's 1,2, and 3 will be assessed every even year
 - ii. PO's 4,5, and 6 will be assessed every odd year

6. Required Institutional Support

- d. Faculty requirements and availability.
 - i. Faculty will have an M.S. and/or Ph.D. with expertise in CS, IT, or related field, and in cybersecurity or information assurance for the risk management and cybersecurity courses.
 - ii. Estimated part-time faculty pay is as follows:
 - First Year: \$32,500
 - Second Year: \$102,500
 - Third Year: \$112,500
 - Fourth Year: \$112,500
- e. Impact on existing programs.

The impact on existing programs is minimal. This new cybersecurity program will allow us to more appropriately relabel the current cybersecurity track in the BSITA program to "Information Assurance". The students will take all of the BSITA courses under the cybersecurity track and will be required to take 5 cybersecurity courses that are exclusively designed for this degree program.
- f. Program director.

Dr. Joe Feliciano
- g. Staff requirements.

Current Full time faculty and adjuncts from the MSIT and BSITA programs will be utilized. There is sufficient faculty with advanced degrees in cybersecurity credentialed in the BSITA and MSIT program to support this degree.
- h. Library resources.
 - i. The ACU Library subscribes to more than 10,000 electronic journals from publishers including Wiley, Springer, ScienceDirect, Oxford, Cambridge, and Brill. Aggregate full-text databases related to cybersecurity include:
 - a. *Applied Science & Technology Source*
 - b. *Business Source Complete*
 - c. *Computer Source*

- d. *eBook Collection (EBSCO)*
- e. *ERIC (EBSCO)*
- f. g. *IEEE Xplore Digital Library*
- g. h. *Information Science & Technology Abstracts*
- h. i. *Lexis-Nexis Universe*
- i. j. *Science & Technology Collection*

ii. All courses are delivered in the Canvas Learning Management System and most, if not all texts and resources are made available electronically through the Canvas course navigation menu. For ACU library resources, each online course has a link to the ACU Library Distance Education Portal and the resources available in the university library.

iii. Students are supported in the use of textbooks and learning resources available in the Canvas LMS by a dedicated team of Student Services Advisors, in addition to the faculty. The ACU Brown Library provides two full-time librarians dedicated to assisting ACU online students.

i. Physical resources.

As an online program, the B.S. in Cybersecurity will require no additional physical resources.

j. Scholarships.

No scholarships will be provided for this program.

k. Recruiting.

Annual costs of \$24,000 are expected.

l. Additional cost to deliver the program.

Category	One-Time	Annual
Faculty	\$0.00	First Year: \$32,500 Second Year: \$102,500 Third Year: \$112,500 Fourth Year: \$112,500
Course Dev.	\$20,000.00	\$0.00
Program Director	\$0.00	Year 1: \$0.00 Year 2+: \$0.00

Staff	\$0.00	\$0.00
Library Resources	\$0.00	\$0.00
Physical Resources	\$0.00	\$0.00
Scholarships	\$0.00	\$0.00
Recruiting/Marketing	\$0.00	\$24,000
TOTAL ADDED COSTS	\$20,000.00	Year 1: \$56,500 Year 2: \$126,500 Year 3 and beyond: \$136,500

7. Additional Information Required for Substantive Changes

a. Student support services.

The Degree in Cybersecurity will be offered through the ACU Dallas which has an established and robust student services model for all students. This model has been uniquely designed to serve the needs of the fully online student population. The student support teams for online programs consist of three distinct student-centered advising roles. These individuals work collaboratively on behalf of groups of students to ensure adequate support and clear lines of communication as issues arise. The student services staff model includes: 1) Admissions Advisors, 2) Student Service Advisors, and 3) Financial Intake Specialists.

These three staff members form a “graduation team” for each enrolled student. These advisors will be trained in the policies, procedures, and protocols associated with the master’s degree. Their mission is to ensure compliance with degree requirements and academic advising for successful degree completion. The specific roles of the Graduation Team member are explained below:

1) Admission Advisors. These individuals partner with students to determine if a program best fits their educational goals. Advisors follow the student throughout the entire application process and answer all questions about programs, forms, fees and everything a student needs to do before beginning the selected program. The advisor also provides students with information on admission requirements and walks students through the process for transfer of credit to ACU.

2) Student Service Advisors. These advisors support students beginning with their first course and ending at graduation. They answer specific questions about setting and maintaining course schedules, program advising issues, and academic support. They work with students through their graduation date addressing student retention and persistence. Student Service Advisors are the students' resource for academic policy and procedure and also provide students with valuable insight concerning resources to assist students throughout their academic program.

3) Financial Intake Specialists. These individuals explain financial options available and help students select a plan that meets their specific needs -- including external grants, scholarships, loans, tuition deferral and other services such as military/veteran benefits. They provide the student with financial expertise throughout the academic experience and are available to answer any financial questions.

These three distinct advisor roles provide committed professionals to walk alongside students in their spiritual and educational journey while supporting ACU's Christian mission. Their commitment is to help students throughout their academic experiences and to guide students in identifying their work as a vocation that contributes to furthering God's purposes for the world. The Graduation Team forms a vital support network for online students and plays an important role in the ongoing work of the university.

Upon enrollment, students in the Cybersecurity program will be provided access to the university catalog and the *ACU Dallas Student Handbook*. The Student Handbook includes web links, email addresses, and phone numbers relating to specific online student needs and available services. Specific examples of these services include:

- The learning management system (LMS) used for all online courses is Canvas. ACU's Team 55 provides technical support for login issues and basic connectivity problems students may experience, as well as issues arising from the LMS. Each Canvas course contains a link connecting online students to Team 55 by phone or email. In addition, Student Service Advisors can provide basic LMS support.
- Students have access to a number of software packages including Google Workspace, Microsoft Office 365, and Adobe Creative Cloud Suite.
- Students can access all materials for their coursework through the online bookstore that was specifically created for ACU online students. This gives students the ability to easily and quickly access required materials for their courses.
- Online students have access to a premium Grammarly account that provides automated paper review and revision. Students have access to Grammarly through Canvas, Microsoft Word and Chrome. The ACU Writing Center Blog houses online APA resources, style guides and articles. Students also have access to Turn-it-in, which provides additional citation support for students.

Further, students will be able to access Tutor.com for course-specific needs including paper review and coaching.

- Students have access to Wildcat Care, an online healthcare benefit that provides 24-hour access to a medical professional. This benefit will allow students to be diagnosed for common medical conditions whether they are at home or traveling.
- Disability services are coordinated through the ACU Alpha Scholars program. Alpha Scholars addresses Disability Services, and learning/testing needs for qualified students. Alpha students receive an assessment of their individual learning styles and study habits and assistance in adapting study strategies to their unique learning characteristics.
- The TAO Self-Help Service is available to all online students and can help students with stress, anxiety, relationship problems, anger management, problem-solving, communication, and evaluation of alcohol and drug use. TAO Self-Help can be used as individual modules for focused problems like problem-solving or communications or can be used as sets of modules for more in-depth help with a problem area.
- The ACU Career Services office is available to all online students through email, telephone, live chat, or video chat. The Career Center provides students with career exploration help, career planning, job and internship postings, career events, interviewing tips, a career resources guide, LinkedIn Profile advice, and a video interviewing system to provide online students with interviewing preparation and advice.
- ACU Students can participate in live teleconferences with our Associate Dean of Vocational Formation where they can explore practices and postures to help individuals endure difficult seasons of work. These 30-minute webinar series will discuss how your everyday work is the very place we can experience meaning, purpose, and participation in communities that flourish. These are held every 7 weeks.
- Upon graduation, students will be eligible for ACU's alumni services and benefits.
- ACU offers free University-wide access to LinkedIn Learning, the online software training library. LinkedIn Learning provides instruction in a wide range of areas including software use, web design, and even speaking skills. Students have access to more than 120,000 video tutorials, more than 400 software titles, and instruction from world-class experts. New content is added each week to the growing support center.

b. Describe financial resources available to support the new program:

First Year Budget

EXPENSE	AMOUNT
---------	--------

Faculty	\$32,500
Program Director	\$0.00
Recruiting.Marketing	\$24,000
Student Services (existing staff)	0.00
TOTAL FIRST YEAR BUDGET	

First Year Revenue

NUMBER OF STUDENTS	NUMBER OF COURSES	ESTIMATED COURSE TUITION	AMOUNT
TOTAL FIRST YEAR REVENUE			

First-Year Cashflow

Revenue	
Expense	
PROFIT/(LOSS)	

- c. Provide contingency plans in the event required resources do not materialize.

As ACU Dallas continues to expand its academic offerings, new programs are funded from existing cash flow from campus operations. ACU Dallas reviews performance data continuously by the Executive Leadership Team throughout the year with weekly reports and monthly reviews with the president of the university and the assistant vice president of university finance. These monthly sessions focus on enrollment, retention, financial performance, and academic program performance and issues. The dean and program directors meet quarterly with the chief operating officer for the campus to review similar data and to provide input regarding performance and operational issues. In addition, the

Executive Leadership Team, the Academic Administration Group, and the directors from Enrollment & Student Services, Marketing, and Information Technology meet following each academic session to review performance, address emerging problems, and to monitor the viability of all programs.

With this level of review, ACU Dallas is poised to make adjustments and to address most issues. In the event a program cannot reach the level of performance needed to sustain the program, ACU Dallas will assess the progress of each individual student enrolled in the program and will design a teach-out plan or, when the student desires, an alternate program.

8. Supporting Documentation

- m. Approval Chart for Curriculum Changes:
- n. Memo of support from the department chair of each department outside the home department that will provide a course for the program.:
- o. When the new program application is complete, provide the full proposal to the following individuals for review. Each will provide a memo to attach to the proposal.:
 - i. Assistant provost for institutional effectiveness and SACSCOC liaison for substantive change review.:
 - ii. Dean of the library for library resources review.:
 - iii. Dean of the college of the program for a statement of commitment to the items in Required Institutional Support.:
 - iv. Assistant provost for curriculum and assessment for review of the program outcomes, curriculum map, and assessment plan and evaluation of compliance with academic policies.:



MEMORANDUM

TO: Academic Council
College of Graduate and Professional Studies

FROM: Nannette W. Glenn, Ph.D., Dean

DATE: May 8, 2023

RE: Required Institutional Support
B.S. Cybersecurity

I have examined the items detailed in the application as required institutional support for the creation, implementation, and maintenance of the new program, Bachelor of Science in Cybersecurity. I hereby acknowledge the obligations of this initiative and commit to providing the institutional support, as set forth.

Nannette W. Glenn, Ph.D.

MEMORANDUM

TO: CGPS Academic Council
FROM: Chris Riley, Associate Provost for Institutional Effectiveness and SACSCOC Liaison
DATE: May 4, 2023
RE: Substantive Change Determination for B.S in Cybersecurity

The purpose of the Substantive Change review process is to determine whether a program change (curricular or otherwise) constitutes a “significant departure” as described by SACSCOC. Based on my review of the information provided for this program including the percentage of new content (12.5%), existing expertise and experience and new resources needed, this does not qualify as a significant departure per SACSCOC guidelines. **Therefore, no substantive change notification or approval is required.**

memo

To: Joe Feliciano
From: Jessica Smith
Date: May 4, 2023
Re: New Program Application — Cybersecurity B.S.

Your work on the Cybersecurity B.S. degree plan has yielded a thorough and thoughtful proposal that will allow students to develop skills in protecting digital infrastructure, providing valuable career opportunities. The program's curriculum appropriate rigor for undergraduate students at the university, pulling from the curriculum already established in information technology administration and adding additional depth.

The program will introduce five new courses. All will need to be approved by your college's academic council before they will be available for a functioning degree audit for your program. They may be introduced beginning at any time and each have the latest deadline for submission in the proposal, so in any case, all courses in this degree plan will be submitted by February 2024.

The course offerings are mapped out well, and the specificity of assessment plan should allow you to continually improve the program. The picture of the need for institutional commitment is clear.

Thank you for your work toward this addition to our curriculum.

ABILENE CHRISTIAN UNIVERSITY
LIBRARY

M E M O R A N D U M

DATE: April 21, 2023
TO: Dr. Joe Feliciano
FROM: Mark McCallon, Library Associate Dean for Library Information Services
RE: New Program Application for Bachelor of Science in Cybersecurity

Thank you for the opportunity to review the new program application for the proposed Bachelor of Science in Cybersecurity.

The Brown Library can provide sufficient resources to support the new program with the agreement that the Library will have the opportunity to review and comment on each new course. This review will be part of the instructional design process.