COLLIN COLLEGE

Program Learning Outcomes and Course Alignment (POCA) for Workforce Programs

Program Name: Bachelor of Applied Technology (BAT) in Cybersecurity

Program Learning Outcomes:	
Program Learning Outcome 1:	Demonstrate Enterprise risk management and mitigation strategies.
Program Learning Outcome 2:	Apply common Cybersecurity industry standards to secure systems.
Program Learning Outcome 3:	Describe common cybersecurity governance practices used in US and International businesses.
Program Learning Outcome 4:	Demonstrate proficiency in the identification, evaluation, and reporting of cyber threats.
Program Learning Outcome 5:	Demonstrate proficiency in security operations to include the remediation and eradication of cyber threats within the Enterprise space.
Program Learning Outcome 6:	Outline, develop, and prepare to implement a purposeful cybersecurity training program.
Program Learning Outcome 7:	Demonstrate proficiency in the use of risk assessments.
Program Learning Outcome 8:	Apply security architecture and related subcomponents.
Program Learning Outcome 9:	Apply cybersecurity analytical tools for appropriate end purposes.

Section I: Technical Courses

For **all technical courses** in the program, indicate how the course will support the program learning outcomes. Include courses outside your discipline area and work collaboratively with those disciplines to determine how the course(s) will support the program learning outcomes.

Please note that it is understandable if these courses do not assess the program learning outcomes and serve predominantly to introduce, practice and/or emphasize the program outcomes.

How to complete the program map:

For example, if course WXYZ 1234 introduces students to one of the program outcomes, then enter "I" for that specific program outcome. Please note that a course can be "I", "P", "E" and/or "A" in any program outcome.

Program Map ▼

I=Introduced P=Practiced E=Emphasized A=Assessed

Program Courses	Program Learning Outcome 1	Program Learning Outcome 2	Program Learning Outcome 3	Program Learning Outcome 4	Program Learning Outcome 5	Program Learning Outcome 6	Program Learning Outcome 7	Program Learning Outcome 8	Program Learning Outcome 9
CPMT-1305				I, P, E					
ITCC-1314				P, E					
ITCC-1344				P, E					
ITMT-1372		I, P, E							
ITMT-1373		P, E							
ITNW-1358				E					
ITSC-1316			I, P, E						
~~ITSE-1359~~ ITSC 1342							~~I, E~~		
ITSY-1300	I, E			P, E		I, E			
ITSY-2300	P, E	P, E	P, E						
ITSY-2301	P, E			P, E	I, P, E				
ITSY-2330	P, E	P, E		P, E	P, E		P, E	I, P, E	I, P
ITSY-2341	P, E, A	P, E, A	P, E, A	P, E	P, E	P, E	P, E, A	P, E, A	E, A

ITSY-2342	P, E				P, E				
ITSY-2343	P	P, E	P, E	P, E	P, E		P, E		
CYBR-3310	P, E							I, P, E	
CYBR-3320	P, E								
CYBR-3330	E			P, E					
CYBR-3340	P, E								
CYBR-3350	P, E								
CYBR-3360	P, E			P, E					
CYBR-4310	P, E	P, E	P, E	P, E	P, E	P, E	P, E	P, E	P, E
CYBR-4320	P, E	P, E,	P, E,	P, E	P, E	P, E	P, E	P, E	P, E
CYBR-4330	P, E	P, E	P, E	P, E	P, E	P, E	P, E	P, E	
CYBR-4340	P, E	P, E	P, E	P, E	P, E	P, E	P, E	P, E	P, E
CYBR-4350	P, E, A	P, E, A	P, E, A	P, E, A	P, E, A	P, E, A	P, E, A	P, E, A	P, E

Developing an Assessment Plan for Program Learning Outcomes

Review existing assessment methods and current practices for collecting/gathering student data to identify direct and indirect methods of assessment. Remember that the data will need to be gathered, analyzed, and used to support the program's continuous improvement processes.

Note: Because courses from other disciplines already have assessment plans in place, they do not have to be included in this assessment plan. Nonetheless, proposers must work collaboratively with these other disciplines to stay current and up-to-date with the assessment plans in these courses.

Describe the direct and indirect assessment methods that will be used to assess the program learning outcomes. Include a) what will be assessed, b) how will it be assessed, c) who will be assessing it, and d) when will it be assessed.

Program-Level Learning Outcome (e.g. Students will describe the impact of various cultures on American cuisine.)	**Assessment Measure(s) and Where Implemented in Curriculum –** Description of Instrument(s)/ process(es) used to measure results and indication of where the assessment will be collected in curriculum. (e.g. Essay on Cultural influences on American cuisine in CUIS 1300.)	**Targets- Level of Success Expected** (e.g. 80% of students score 2.5 or better on rubric for essay on cultures and cuisine.)
Demonstrate Enterprise risk management and mitigation strategies.	**AAS Level Assessment**: In the Final Project in ITSY 2341 Security Management Practices students research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the AAS Program. This does not address the risk assessment/classification for the organization – this focuses on remediation/management/mitigation. During this project students are assessed on their use of Enterprise Risk Management/Mitigation using a scenario in which students create an enterprise risk management plan. This plan is broad in suggesting risk management/mitigation strategies to include: Identification/Application of appropriate security frameworks, GAP analysis, RACI matrix provides, authorization/delegation of responsibilities, data classification scheme(s), magnetic remanence schema, overall risk management Program, and high-risk mitigation plan/strategy. **BAT Level Assessment**: In the Final Project in CYBR 4350 (Capstone): During the capstone project, students create, implement, and recommend for remediation a working Enterprise Information/Cyber Security and Risk Program to address all aspects of risk, addressed throughout the BAT program. This project was faculty-developed to include PCI, PHI, and FERPA components. Students are assessed on their implementation of technology to fulfill enterprise requirements, defense of their	75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. 75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO.

	frameworks/decisions during an enterprise audit, and their remediation plan to correct deficiencies disclosed during an audit of their implemented program.	
Apply common Cybersecurity industry standards to secure systems.	**AAS Level Assessment:** In the Final Project in ITSY 2341 Security Management Practices students research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the AAS Program. During this project students are assessed on their application of cybersecurity industry standards (to include methods & frameworks) using a faculty developed rubric detailing technical and administrative policy usage. **BAT Level Assessment**: In the Final Project in CYBR 4350 (Capstone): Students create, implement, and recommend for remediation a working Enterprise Information/Cyber Security and Risk Program to address all aspects of risk, addressed throughout the BAT program. During this project students are assessed on their ability to identify, implement, and maintain the appropriate organizational security posture based upon selecting the correct standards and methodologies.	75% of students score 80% or above on project ITSY 2341 rubric elements aligned with this PLO. 75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO.
Describe common cybersecurity governance practices used in US and International businesses.	**AAS Level Assessment**: In the Final Project in ITSY 2341 Security Management Practices students research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the AAS Program. During this project students are assessed using a faculty developed rubric covering multiple aspects of governance, specifically who within the organization is responsible for governance, how risk is evaluated, and finally how does the governance align with the overall business structure and business requirement(s). **BAT Level Assessment**: As part of the Capstone Project in CYBR 4350 students	75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. 75% of students score 80% or above on CYBR 4350 project rubric

	research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the BAT Program. Students are assessed on their implementation of their program using common governance techniques learned throughout the entire BAT program.	elements aligned with this PLO.
Demonstrate proficiency in the identification, evaluation, and reporting of cyber threats.	**BAT Level Assessment**: In the Final Project in CYBR 4350 (Capstone): Students create, implement, and recommend for remediation a working Enterprise Information/Cyber Security and Risk Program to address all aspects of risk, addressed throughout the BAT program. During this project students are assessed on how they identify, evaluate and report cyber threats by requiring the inclusion of threat collection and identification strategies using Threat Intelligence feeds, IoC (Indicators of Compromise) identification, event detection, investigation of event, evaluation of event to determine incident response, escalation of attack status, and reporting techniques used to alert leadership of cyber threat.	75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO.
Demonstrate proficiency in security operations to include the remediation and eradication of cyber threats within the Enterprise space.	**BAT Level Assessment**: In the Final Project in CYBR 4350 (Capstone): Students create, implement, and recommend for remediation a working Enterprise Information/Cyber Security and Risk Program to address all aspects of risk, addressed throughout the BAT program. During this project students are assessed using a faculty developed rubric that measures the strength of their threat containment plan (including use/misuse cases), management, and eradication techniques.	75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO.
Outline, develop, and prepare to implement a purposeful cybersecurity training program.	**BAT Level Assessment**: In the Final Project in CYBR 4350 (Capstone): Students create, implement, and recommend for remediation a working Enterprise Information/Cyber Security and Risk Program to address all aspects of risk, addressed throughout the BAT program. Students are assessed on their ability to create an organizationally specific	75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO.

	user training program as part of their enterprise security plan.	
Demonstrate proficiency in the use of risk assessments.	**AAS Level Assessment**: In the Final Project in ITSY 2341 Security Management Practices students research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the AAS Program. During this project students are assessed on their ability to perform a risk assessment from a descriptive point of view, using a faculty-guided and student-designed framework that builds the foundation for the enterprise. Students are assessed on their ability to identify common risks, plan risk assessments, and describe how different types of risk assessments function as a part of the overall risk stance of the organization. Additionally, students describe how this is to be presented to leadership as part of the enterprise risk assessment process. **BAT Level Assessment**: In the Final Project in CYBR 4350 (Capstone) students create, implement, and recommend for remediation a working Enterprise Information/Cyber Security and risk program which includes a requirement for regularly scheduled vulnerability assessments combined with a requirement to plan for mitigation of vulnerabilities. Students are assessed on their ability to identify whether a vulnerability assessment will occur internally or externally, whether by internal assets or outsourced, and frequency of testing. Additionally, students will have to identify which systems/ components cannot be tested and why.	75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. 75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO.
	AAS Level Assessment: In the Final Project in ITSY 2341 Security Management Practices students research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the AAS Program. During the AAS	75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO.

Apply security architecture and related subcomponents.	degree we assess security architecture from a descriptive point of view, using a faculty guided and student designed framework that builds the foundation for the Enterprise security architecture. During this project students are assessed on their identification of needs for the overall security architecture including how different components interact to either enhance or weaken the overall security posture of the organization. Students are not required to implement at this level as this is part of the Capstone project during their final course in the BAT degree. **BAT Level Assessment**: In the Final Project in CYBR 4350 (Capstone) students create, implement, and recommend for remediation a working Enterprise Security Architecture. Students are required to design and build an enterprise network using industry best practices specific to the technology they are implementing (CIS controls for Servers, Routers, and Switches). Students are assessed on their implementation of security architecture that was previously recommended per industry standards.	75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO.
Apply cybersecurity analytical tools for appropriate end purposes.	**AAS Level Assessment**: In the Final Project in ITSY 2341 Security Management Practices students research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the AAS Program. Students are assessed on the use of basic analysis tools/techniques using RACI matrixes and association matrixes within the context of the Enterprise cyber risk program.	75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO.