**Continuous Improvement Plan**

**Date:** Spring 2024 **Name of Program/Unit:** Bachelor of Applied Technology in Cybersecurity

**Contact name:** Dr. James E. Freedle II **Contact email:** jfreedle@collin.edu **Contact phone:**  (972) 578-5546

**Table 1: CIP Outcomes, Measures & Targets Table (focus on at least one for the next two years)**

|  |  |  |
| --- | --- | --- |
| **A. Expected Outcome(s)**Results expected in this unit(e.g. Authorization requests will be completed more quickly; Increase client satisfaction with our services) |  **B. Measure(s)**Instrument(s)/process(es) used to measure results(e.g. survey results, exam questions, etc.)Include Course Information and Semester in which assessment will occur | **C. Target(s)**Level of success expected(e.g. 80% approval rating, 10 day faster request turn-around time, etc.) |
| 1) Securely Provision (SP) -Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development. | Skills-based Assessment | Project based evaluation / Skills Based Assessment (SBA) (may be physical, virtual, or online lab based):Overall reduction of 75% of general system vulnerabilities for Operating System (OS) (internal - default install), Systems should not contain vulnerabilities with known remediations that have been posted for more than 3 months. Overall reduction of 90% for firewall vulnerabilities is normal (perimeter) based upon initial values per systems (includes Geofencing & domain filtering) |
| Outcome #1 Demonstrate Enterprise risk management and mitigation strategies. | 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:1. Administrative and technical controls introduced/practiced during the AAS and BAT Programs
2. PCI, PHI, and FERPA components
3. Students are assessed on their implementation of technology to fulfill enterprise requirements
4. Defense of their frameworks/decisions during an enterprise audit.

A remediation plan to correct deficiencies disclosed during an audit of their implemented program. | 75% of students score 80% or above on CYBR-4350 project rubric elements aligned with this Program Level Outcome |

**Description of Fields in the Following CIP Tables:**

**A. Outcome(s)** -Results expected in this program (e.g. Students will learn how to compare/contrast conflict and structural functional theories; increase student retention in Nursing Program).

**B. Measure(s)** -Instrument(s)/process(es) used to measure results

(e.g. results of surveys, test item questions 6 & 7 from final exam, end of term retention rates, etc.)

**C. Target(s)** -Degree of success expected (e.g. 80% approval rating, 25 graduates per year, increase retention by 2% etc.).

**D. Action Plan** -Based on analysis, identify actions to be taken to accomplish outcome. What will you do?

**E. Results Summary** - Summarize the information and data collected in year 1.

**F. Findings** - Explain how the information and data has impacted the expected outcome and program success.

**G. Implementation of Findings** – Describe how you have used or will use your findings and analysis of the data to make improvements.

**Table 2. CIP Outcomes 1 & 2 (FOCUS ON AT LEAST 1)**

|  |
| --- |
| 1. **Outcome #1** Demonstrate Enterprise risk management and mitigation strategies.
 |
| 1. **Measure (Outcome #1)**

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:1. Administrative and technical controls introduced/practiced during the AAS and BAT Programs
2. PCI, PHI, and FERPA component
3. Students are assessed on their implementation of technology to

fulfill enterprise requirements1. Defense of their frameworks/decisions during an enterprise audit
2. A remediation plan to correct deficiencies disclosed during an

audit of their implemented program. | 1. **Target (Outcome #1)**

75% of students score 80% or above on CYBR-4350 project rubric elements aligned with this Program Level Outcome |
| 1. **Action Plan (Outcome #1)**

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 frameworks/decisions during an enterprise audit, and their remediation plan to correct deficiencies disclosed during an audit of their implemented program. |
| 1. **Results Summary (Outcome #1)**

 |
| 1. **Findings (Outcome #1)**

While the number of students increased from 2022 to 2023, with 2 students withdrawing form the course, the average course GPA increased from 3.97 to 3.99. |
| 1. **Implementation of Findings**

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.  |

|  |
| --- |
| 1. **Outcome #2** Apply common Cybersecurity industry standards to secure systems.
 |
| 1. **Measure (Outcome #2)**

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, based upon selecting the correct standards and methodologies, on their ability to:1. Identify
2. Implement
3. Maintain the appropriate organizational security posture.
 | 1. **Target (Outcome #2)**

75% of students score 80% or above on CYBR-4350 project rubric elements aligned with this PLO. |
| 1. **Action Plan (Outcome #2)**

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. |
| 1. **Results Summary (Outcome #2)**

 |
| 1. **Findings (Outcome #1)**

While the number of students increased from 2022 to 2023, with 2 students withdrawing form the course, the average course GPA increased from 3.97 to 3.99. |
| 1. **Implementation of Findings**

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 |

**Program Assessment Data Report**

 **Program: Bachelor of Applied Technology in Cybersecurity Terms Data Collected: Fall 2022-Fall 2023**

|  |  |  |  |
| --- | --- | --- | --- |
| Program-Level Learning Outcome- (From Assessment Plan) | Assessment Measure(s) and Where Implemented in Curriculum – (From Assessment Plan) | Targets- Level of Success Expected-(From Assessment Plan) | Assessment Results – (Provide Data in a form related to targeted levels of success to left. Indicate if Targeted level of success was met, partially met, or not met.) |
| Demonstrate Enterprise risk management and mitigation strategies. | 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 frameworks/decisions during an enterprise audit, and their remediation plan to correct deficiencies disclosed during an audit of their implemented program. | 75% of students score 80% or above. | 99% of students complete the course scoring 80% or better. |
| Apply common Cybersecurity industry standards to secure systems. | 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. | 99% of students complete the course scoring 80% or better. |
| Describe common cybersecurity governance practices used in US and International businesses. | As part of the Capstone Project in CYBR 4350 students 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. | 75% of students score 80% or above. | 99% of students complete the course scoring 80% or better. |
| Demonstrate proficiency in the identification, evaluation, and reporting of cyber threats. | 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. | 99% of students complete the course scoring 80% or better. |
| Demonstrate proficiency in security operations to include the remediation and eradication of cyber threats within the Enterprise space. | 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. | 99% of students complete the course scoring 80% or better. |
| Outline, develop, and prepare to implement a purposeful cybersecurity training program. | 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 user training program as part of their enterprise security plan.  | 75% of students score 80% or above. | 99% of students complete the course scoring 80% or better. |
| Demonstrate proficiency in the use of risk assessments. | 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. | 99% of students complete the course scoring 80% or better. |
| Apply security architecture and related subcomponents. | 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. | 99% of students complete the course scoring 80% or better. |