**Continuous Improvement Plan**

**Outcomes might not change from year to year. For example, if you have not met previous targets, you may wish to retain the same outcomes. *If this is an academic, workforce, or continuing education program, you must have at least one student learning outcome.* You may also add short-term administrative, technological, assessment, resource or professional development goals, as needed.**

**Date:** Jan 2022 **Name of Program/Unit:** CyberSecurity

**Contact name:** Ervin Frenzel **Contact email:** efrenzel@collin.edu **Contact phone:**  469-365-1936

**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.) | **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 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, and port reduction/isolation). |
| **Outcome #1** Demonstrate Enterprise risk management and mitigation strategies. | (ITSY 2341)  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:   1. Identification/Application of appropriate security frameworks 2. GAP analysis 3. RACI matrix provides 4. authorization/delegation of responsibilities 5. data classification scheme(s) 6. magnetic remanence schema 7. overall risk management Program 8. high-risk mitigation plan/strategy   (CYBR 4350)  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 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. |

**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)**   (ITSY 2341)  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:   1. Identification/Application of appropriate security frameworks 2. GAP analysis 3. RACI matrix provides 4. authorization/delegation of responsibilities 5. data classification scheme(s) 6. magnetic remanence schema 7. overall risk management Program 8. high-risk mitigation plan/strategy   (CYBR 4350)  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 5. 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 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. |
| **Action Plan (Outcome #1) -** 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 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)**   AAS results:    Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #1)**   Current capstone participants are within the acceptable range (AAS – ITSY 2341):    Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   As, current capstone participants are within the acceptable range, programmatically we will be adding additional security implementations into the Capstone projects (such as a full implementation of CIS level 2 controls). Additionally, we will be increasing the percentage from 75% to 80% of successful completers. | |

|  |  |
| --- | --- |
| 1. **Outcome #2** Apply common Cybersecurity industry standards to secure systems. | |
| 1. **Measure (Outcome #2)**   (ITSY 2341)  Using a faculty developed rubric detailing technical and administrative policy usage, students are assessed on their application of cybersecurity industry standards (to include methods & frameworks).  (CYBR 4350)  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 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. |
| **Action Plan (Outcome #2) -** 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. | |
| 1. **Results Summary (Outcome #2)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #2)**   Current capstone participants are within the acceptable range (AAS – ITSY 2341):    Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   As, current capstone participants are within the acceptable range, programmatically we will be adding additional security implementations into the Capstone projects (such as a full implementation of CIS level 2 controls). Additionally, we will be increasing the percentage from 75% to 80% of successful completers. | |

|  |  |
| --- | --- |
| 1. **Outcome #3** Describe common cybersecurity governance practices used in US and International businesses. | |
| 1. **Measure (Outcome #3)**   (ITSY 2341)  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:   1. Governance, specifically who within the organization is responsible for governance 2. how risk is evaluated 3. how does the governance align with the overall business structure and business requirement(s)   (CYBR 4350)  Students are assessed on their **implementation** of their program using common governance techniques learned throughout the entire BAT program.   1. Governance, specifically who within the organization is responsible for governance 2. how risk is evaluated 3. how does the governance align with the overall business structure and business requirement(s) | 1. **Target (Outcome #3)**  * 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. |
| **Action Plan (Outcome #3) -** 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. 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 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. | |
| 1. **Results Summary (Outcome #3)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #3)**   Current capstone participants are within the acceptable range (AAS – ITSY 2341):    Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   As, current capstone participants are within the acceptable range, programmatically we will be adding additional security implementations into the Capstone projects (such as a full implementation of CIS level 2 controls). Additionally, we will be increasing the percentage from 75% to 80% of successful completers. | |

|  |  |
| --- | --- |
| 1. **Outcome #4** Demonstrate proficiency in the identification, evaluation, and reporting of cyber threats. | |
| 1. **Measure (Outcome #4)**   (CYBR 4350)  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 to alert leadership.  During this project students are assessed on how they:   1. Identify 2. Evaluate 3. Report   Cyber threats by requiring the inclusion of threat collection and identification strategies using:   1. Threat Intelligence feeds 2. IoC (Indicators of Compromise) identification 3. event detection 4. investigation of event 5. evaluation of event to determine incident response 6. escalation of attack status 7. reporting techniques | 1. **Target (Outcome #4)**  * 75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO. |
| **Action Plan (Outcome #4) -** Enterprise risk management and mitigation strategies.  **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. | |
| 1. **Results Summary (Outcome #4)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #4)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |

|  |  |
| --- | --- |
| 1. **Outcome #5** Demonstrate proficiency in security operations to include the remediation and eradication of cyber threats within the Enterprise space. | |
| 1. **Measure (Outcome #5)**   (CYBR 4350)  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. | 1. **Target (Outcome #5)**  * 75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO. |
| **Action Plan (Outcome #5) -** Enterprise risk management and mitigation strategies  **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. | |
| 1. **Results Summary (Outcome #5)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #5)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |

|  |  |
| --- | --- |
| 1. **Outcome #6** Outline, develop, and prepare to implement a purposeful cybersecurity training program. | |
| 1. **Measure (Outcome #6)**   (CYBR 4350)  Students are assessed on their ability to create an organizationally specific user training program as part of their enterprise security plan. | 1. **Target (Outcome #6)**  * 75% of students score 80% or above on CYBR 4350 project rubric elements aligned with this PLO. |
| **Action Plan (Outcome #6) -** 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. 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, work together to resolve issues, 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 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. | |
| 1. **Results Summary (Outcome #6)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #6)**   Current capstone participants are within the acceptable range (AAS – ITSY 2341):    Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   As, current capstone participants are within the acceptable range, programmatically we will be adding additional security implementations into the Capstone projects (such as a full implementation of CIS level 2 controls). Additionally, we will be increasing the percentage from 75% to 80% of successful completers. | |

|  |  |
| --- | --- |
| 1. **Outcome #7** Demonstrate proficiency in the use of risk assessments. | |
| 1. **Measure (Outcome #7)**   (ITSY 2341)  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:   1. identify common risks 2. plan risk assessments 3. describe how different types of risk assessments function as a part of the overall risk stance of the organization 4. describe how this is to be presented to leadership as part of the enterprise risk assessment process.   (CYBR 4350)  Students create, implement, and recommend for remediation a working Enterprise Information/Cyber Security and risk program which includes:   1. a requirement for regularly scheduled vulnerability assessments 2. a requirement to plan for mitigation of vulnerabilities 3. their ability to identify whether a vulnerability assessment will occur internally or externally 4. Identifying who will conduct audits 5. frequency of testing 6. identify which systems/ components cannot be tested and why. | 1. **Target (Outcome #7)**  * 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. |
| **Action Plan (Outcome #7) -** 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. 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. | |
| 1. **Results Summary (Outcome #7)**   Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #7)**   Current capstone participants are within the acceptable range (AAS – ITSY 2341):    Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   As, current capstone participants are within the acceptable range, programmatically we will be adding additional security implementations into the Capstone projects (such as a full implementation of CIS level 2 controls). Additionally, we will be increasing the percentage from 75% to 80% of successful completers. | |

|  |  |
| --- | --- |
| 1. **Outcome #8** Apply security architecture and related subcomponents. | |
| 1. **Measure (Outcome #8)**   (ITSY 2341)  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  (CYBR 4350)  Students create, implement, and recommend for remediation a working Enterprise Security Architecture. | 1. **Target (Outcome #8)**  * 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. |
| **Action Plan (Outcome #8) -** Enterprise risk management and mitigation strategies.  Students research and create an Enterprise Information/Cyber Security and Risk Program to address all administrative and technical controls introduced/practiced during the Program. In CYBR 4350 students create, **implement, and recommend for remediation a working** Enterprise Security Architecture.  **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 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. | |
| 1. **Results Summary (Outcome #8)**   For the AAS, 92.86% of students meet expectations with 7.14% needing to improve. As a Department we are expanding the Capstone (AAS – ITSY 2341 to encompass greater security requirements – including programmatically including Industry standards such as CIS (lvl 2) and SOC lvl 2.  Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #8)**   Current capstone participants are within the acceptable range (AAS – ITSY 2341):    Currently there are no results summary or findings for the BAT program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   As, current capstone participants are within the acceptable range, programmatically we are adding additional security implementations/content into the Capstone projects (such as a full implementation of CIS level 2 controls). Additionally, we will be increasing the percentage from 75% to 80% of successful completers. | |

|  |  |
| --- | --- |
| 1. **Outcome #9** Apply cybersecurity analytical tools for appropriate end purposes. | |
| 1. **Measure (Outcome #9)**   (ITSY 2341)  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. | 1. **Target (Outcome #9)**   75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. |
| **Action Plan (Outcome #9) -** 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. 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. | |
| 1. **Results Summary (Outcome #9)**   Currently there are no results summary or findings for the AAS program as the first iteration of students has not completed the program. | |
| 1. **Findings (Outcome #9)**   Currently there are no results summary or findings for the AAS program as the first iteration of students has not completed the program. | |
| 1. **Implementation of Findings**   Currently there are no results summary or findings for the AAS program as the first iteration of students has not completed the program. | |