**Continuous Improvement Plan**

**Date:** Spring 2024 **Name of Program/Unit:** Information Systems Cybersecurity - AA

**Contact name:** Nadia Bilal **Contact email:** Nbilal@collin.edu **Contact phone:**  972-378-8737

**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 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. | (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. |

**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. |
| **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. | |
| 1. **Results Summary (Outcome #1)**   AAS results ITSY 2341: | |
| 1. **Findings (Outcome #1)**   We increased the percentage from 89% to 95% of successful completers until 2023 and expecting to improve in the upcoming years. | |
| 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)**   (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). | **C Target (Outcome #2)**   * 75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. |
| 1. **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. | |
| 1. **Results Summary (Outcome #2)**   For the AAS, 94% of students completed the AAS degree, with 6% needing to improve to graduate between 2019-2023. As a department, we are expanding the Capstone (AAS – ITSY 2341 to encompass more significant security requirements – including programmatically, Industry standards such as CIS (level 2) and SOC level 2. | |
| 1. **Findings (Outcome #1)**   Current capstone participants are within the acceptable range (AAS – ITSY 2341): | |
| 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 increased the percentage of successful completers from 89% to 95% until 2023 and expect to improve in the upcoming years. | |

|  |  |
| --- | --- |
| 1. **Outcome #3**   Learn various types of vulnerabilities, malicious activity, mitigation techniques. | |
| 1. **Measure (Outcome #3)**   **ITSY1300**  Students will Compare and contrast various types of security controls, summarize fundamental security concepts, common threat vectors and attack surfaces, various types of vulnerabilities and mitigation techniques used to secure the enterprise. | **C Target (Outcome #3)**   * 75% of students scored 80% or above on ITSY 1300 |
| 1. **Action Plan (Outcome #3)**   **AAS Level Assessment:**  Students who complete ITSY 1300 will be more resilient to cybersecurity threats and vulnerabilities because they will have the fundamental knowledge and abilities needed to safeguard IT systems, networks, and applications. | |
| 1. **Results Summary (Outcome #3)**   For the AAS, 95% of students completed the ITSY 1300, with 5% needing to improve between 2019-2023. | |
| 1. **Findings (Outcome #3)** | |
|  | |

**Program Assessment Data Report**

**Program: Information Systems – Cybersecurity – AA Terms Data Collected: 2022- 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.) |
| Students will be able to demonstrate the knowledge of Information Security, ethics, legal environment, vulnerabilities, threat types and countermeasures. Hand on practice Lab will be required for better learning and understanding. | In ITSY 1300 Students will be working on Activities and labs like "managing password security, "which will encourage students to study for the rest of their lives and pursue cybersecurity careers. Every module will have reflection discussions, peer responses, Quizzes, and prompts to promote introspection and candid communication among peers. | 75% of students will score 80% or above. | 95% of students complete the course scoring 87% or better. |
| Students will use open-source role to discover threat intelligence and organizational incident response. Topics include collection methods, management of operations, classification, production and analysis, assessment of threat vulnerability, business impact analysis, incidence response, and identification of various reporting requirements. The use of link diagrams and various types of association matrices will be introduced and emphasized. | In ITSY 1371**,**Students will use OSINT tools and discover how these can be used to supplement organizational collection plans. Students will watch videos for understanding and will be measured through Assignments, Labs, and Discussions with peer responses. They will also use the grid matrix to identify the factors that could provide information about the organization without violating privacy and can present their work in the form of presentation. | 75% of students will score 75% or above. | 87% of students complete the course scoring 75% or better. |
| 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. | 94% of students complete the course scoring 91% or better. |
| 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. | 75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. | 94% of students complete the course scoring 91% or better. |
| 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. |  | 94% of students complete the course scoring 91% or better. |
| 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 | 75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. | 94% of students complete the course scoring 91% or better. |
| 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 | 75% of students score 80% or above on ITSY 2341 project rubric elements aligned with this PLO. | 94% of students complete the course scoring 91% or better. |
| Apply security architecture and related subcomponents. | **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. | 75% of students will score 80% or above. | 94% of students complete the course scoring 91% or better. |