Annual Assessment Report for Academic Programs

The University Assessment Team advocates for the enhancement of student learning through purposeful, meaningful, and feasible student-outcomes assessment practices. The Assessment Team seeks to collaborate with programs, departments, and units to ensure that effective assessment of student learning occurs across the University. To assist in meeting this goal, the Team requests that you complete this Annual Assessment Report form to document student learning in your program. A PDF version of this completed form will be posted to the Academic Affairs Assessment website. Please note that this Annual Assessment Report form should only be completed after you have an Assessment Plan for Academic Programs forms on file with the University Assessment Team. The plan is completed once and only updated when revisions have been made to components of the plan.

1. Degree Level and Program Name: MS in Cybersecurity Management

2. College/School: College of Humanities, Arts & Social Sciences

3. Assessment Overview - Briefly share how student learning outcomes assessment is conducted within your program/department (e.g. number of outcomes, examples of assignments used, and frequency of assessment).

The MS in Cybersecurity Management program has five student learning outcomes, with two outcomes assessed each year. Faculty assess student learning outcomes using direct measures from embedded assignments (e.g. hands-on technical labs, exam questions, design cases, and projects using rubrics).

4. Student Learning Outcomes -Which student learning outcome(s) from the assessment plan filed with the University Assessment Team is/are being reported on in this report? Include the corresponding benchmark(s) for each outcome.

Two student learning outcomes are being assessed in this cycle:

Student Learning Outcome #3: Demonstrate an understanding of the key concepts of information security governance and risk management to include best practices in disaster recovery planning and business continuity. Students will demonstrate an understanding of continuity management based on risk analysis. Students will explain how decisions about criticality factors into contingency planning and state the tradeoff and how those decisions are influenced by likelihood, impact, and the tangible outcome.

Student Learning Outcome #5: Apply security principles and practices to the organizational environment, hardware, software, and human aspects of a system. Students will be able to demonstrate knowledge of secure boot by explaining secure boot, why secure boot is necessary (e.g., what type of adversarial attacks does secure boot prevent), and explaining the load sequence where secure boot is involved in the startup process.

The benchmark for success is to have at least 75% of the students earn a rubric equivalent total score of C or better on final exam essay questions.

5. Institutional Outcomes - For which institutional outcome(s) do the reported student learning outcome(s) align?

SLO Outcome Alignment	Institutional Outcome
Yes	I. Jesuit & Mercy Values
	II. Diversity & Cultural Awareness
Yes	III. Critical Thinking & Problem Solving
	IV. Communication
Yes	V. Professionalism
	VI. Lifelong Learning

6. **Assessment Period:** Select the academic year for which you are reporting results (i.e. when data were collected):

2023-2024

7. **Results, Planned Actions, and/or Actions Taken** -Briefly summarize the assessment results, how they relate to benchmark(s), and how you are using them to enhance student learning and improve program quality.

Outcome #3: 82% (9/11) of the CYBE 5790, Cybersecurity Control Processes students earned a rubric equivalent score of C or better on a final exam essay question, which is above the 75% benchmark for the group of students. The aggregate mean rubric scores (using a 5-point scale) indicated students' strengths were in understanding and discussing the criticality factors and its role in contingency planning. Students' opportunities for improvement were in developing depth and addressing potential impacts, tradeoffs, and outcomes.

Outcome #5: 64% (7/11) of the CYBE 5750, Cybersecurity Technologies students earned a rubric equivalent score of C or better on the final exam essay question, which is below the 75% benchmark for the group of students. The aggregate mean rubric scores (using a 5-point scale) indicated students' strengths were in demonstrating an understanding of security boot and adversarial attacks. Areas for opportunities for improvement include the specific boot and load sequence.

Responding the results of both outcomes, the department reviewed and revised instructional materials and lab assignments to improve student competencies in the identified areas.

Attachment(s):

None