



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 Cybercrime
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 Cybercrime program has five student learning outcomes, with two outcomes assessed each year. Faculty assess use of hands-on, experiential learning technical lab assignments, exams, service-learning assignments, individual and group projects, written reports and a comprehensive research project that will require students to demonstrate the cumulative knowledge, skills and abilities learned throughout the program.

4. **Student Learning Outcomes & Benchmarks** -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.

SLO#1: Possess the capacity to evaluate, develop and implement a legally sufficient and technology-based solution(s) to address cybercrime requirements in the context of the disciplinary standards of criminal justice, cybersecurity and digital forensics. The benchmark for SLO #1 – at least 75% of the students earn a rubric equivalent total score of B or better on a 6–8-page essay paper assignment.

SLO#2: Have the ability to identify an emerging cybercrime problem, then analyze, develop and implement an appropriate law enforcement response and technological-based solution, focused on prevention, response, mitigation and resolution. The benchmark for SLO #2 – at least 75% of the students earn a rubric equivalent total score of B or better on a 6–8-page essay paper assignment.



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

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

6. **Assessment Period:** Select the academic year for which you are reporting results (i.e. when data were collected):
2025-2026

7. **Program Assessment Results** -Briefly summarize the assessment results and how they relate to benchmark(s).

Outcome#1: 78% (7/9) of the Fall 2025_CYCR5400, Cyber Criminology students earned a rubric equivalent score of B or better on a 6–8-page essay paper. The aggregate mean rubric scores, using a 20-point scale, indicated students' strength in their ability to identify a cybercrime incident, evaluate Wall's four category typology identification with subcategories and provide an analysis explaining the chosen typology's fit. The weaknesses in the students who fell short were lack of meaningful depth in their analysis and requirement of 5+ scholarly sources not met. The 78% score exceeded expected level of 75%.

Outcome#2: 83% (5/6) of the Fall 2025_CYCR5770_Cyber Defense Operations students earned a rubric equivalent score of B or better on a 6–8-page opinion paper. The aggregate mean rubric scores, using a 20-point scale, indicated students' strength in identifying and using excellent academic sources, defining privacy and security in the context of cyber defense well, and clearly stating their position. The weakness in the student who fell short was the inability to articulate a clear opinion, incompleteness with vague definitions and sources referencing ChatGPT. The 83% score exceeded the expected level of 75%.

8. **Planned Actions and/or Actions Taken in Response to Assessment Results** - Briefly summarize how you are using the assessment results to enhance student learning and improve program quality.

MS in Cybercrime: In response to the assessment results, the department will review the identified areas and incorporate additional resources to improve student performance.