Cybercrime, Graduate, MS, Tampa

Cip Code: 45.0401

Assessment Cycle: 2019 Reporting **Overall Review:** Report Approved COMPLIANT

Mission Statement

The MS in Cybercrime is a practitioner-oriented academic program that prepares professionals to fight the global threat of cybercrime. Criminal investigators need training that goes beyond the high-tech skills required for cybersecurity professionals. Students experience a comprehensive program of study necessary to gain the skills required by this field of practice. It blends a traditional criminological foundation with STEM-based skills in the study of high-tech criminal investigations, practices and procedures, and tools and methodologies of investigation. This MS degree program provides students with a foundational understanding of key concepts associated with cybercrime, laws and legislation, criminal investigations, and the processing and handling of digital evidence.

Unlike other cyber programs, the MS in Cybercrime is designed and geared toward criminal investigators, not computer scientists. The program is self-contained in terms of computer science skills. Students receive necessary training within the program. There is neither a computer science prerequisite nor required courses in the computer sciences.

Goal 1: Other (non-ALC)

DISCIPLINE-SPECIFIC KNOWLEDGE AND SKILLS – LEGAL FOUNDATION. Students earning a graduate degree in Cybercrime will develop a basic legal foundation related to the enforcement of criminal statutes and investigations of violations of law in the realm of illicit activities generally known as cybercrime.

1a. Student Learning Outcome Statement

Audit Review: AC

Students will demonstrate an understanding of the adaptation and application of search and seizure laws to emerging digital technologies, as well as legislative efforts to balance protections of privacy rights with the need to conduct criminal investigations.

1b. Method of Assessment

Audit Review: AC

Cybercrime faculty have developed a large test bank of multiple choice and true/false questions that address the students' comprehension and understanding of key concepts and applications related to cybercrime law. Questions randomly drawn from the test bank are administered to students in CJE 6690 two times during the 8-week term in which they take the course. The percentage of correct responses on each of the questions will be determined. Analysis of the results and their trend over time will help assess student performance and guide the development of future course materials.

1c. Performance Targets

Audit Review: AC

Success will be demonstrated by at least 70% of the students scoring 80% correct responses or better on each of the two assessments in CJE 6690.

1d. Assessment Results

Audit Review: AC

The following results are for the Spring 2019 term of CJE 6690:

Spring2 2019	N	High Score	Low Score	Average	# Above 80%	% Above 80
Quiz #1	22	100	73	88	20	91%
Quiz #2	22	98	60	83	15	75%

Performance targets were met.

1e. Use of Assessment Results *Audit Review: AC*

The topics covered in CJE 6690 are progressively more technical and complex throughout the first six weeks and then concludes with more general applications of the materials. Each assessment unit (quiz) assumes a full understanding of previous materials and the ability to engage in application at more complex levels in subsequent units.

As the complexity increases in the second assessment unit there is an apparent drop in the number of students scoring 80% or better. Instructors should work more closely with students to ensure they fully understand the prior materials and facilitate their application in more complex levels of operation.

The course topics associated with lower performance items will receive additional attention in the development of future teaching plans.

Plan Review Comments

Report Review Comments

Goal 2: Other (non-ALC)

DISCIPLINE-SPECIFIC KNOWLEDGE AND SKILLS – CRIME SCENE. Students earning a graduate degree in Cybercrime will be able to recognize and identify potential sources of electronic evidence, provide a knowledgeable response to an electronic crime scene, and safely and methodically preserve and collect items of evidentiary value to be used in legal proceedings.

1a. Student Learning Outcome Statement *Audit Review: AC*

Students will demonstrate a comprehension of the identification, collection, acquisition, authentication, preservation, examination, analysis, and presentation of evidence for prosecution purposes to include legal and evidentiary considerations in the field and the courtroom, foundations of digital forensics, and the application of forensic science to digital technologies and digital crime scenes.

1b. Method of Assessment *Audit Review: AC*

Cybercrime faculty have developed a large test bank of multiple choice and true/false questions that address the students' comprehension and understanding of key concepts and applications related to cyber-related crime scenes and digital evidence. Questions randomly drawn from the test bank are administered to students in CJE 6627 two times during the 8-week term in which they take the course. The percentage of correct responses on each of the questions will be determined. Analysis of the results and their trend over time will help assess student performance and guide the development of future course materials.

1c. Performance Targets *Audit Review: AC*

Success will be demonstrated by at least 70% of the students scoring 80% correct responses or better on each of the two assessments in CJE 6627.

1d. Assessment Results *Audit Review: AC*

The following results are for the Spring 2019 term of CJE 6627:

Spring2 2019	N	High Score	Low Score	Average	# Above 80%	% Above 80
Quiz #1	21	96	72	88	18	86%
Quiz #2	21	98	64	88	19	90%

Performance targets were met.

1e. Use of Assessment Results *Audit Review: AC*

The topics covered in CJE 6627 are diverse and there is less reliance on a cumulative understanding and application as the course progresses. The minimal variation between the scores in the two assessments appears to reflect this situation where subsequent course materials are not dependent upon a full and comprehensive understanding of materials presented earlier in the course.

Instructors should work more closely with students to ensure that course topics associated with lower performance items are better and more fully understood. In addition, such items should receive additional attention in the development of future teaching plans.

Plan Review Comments

Report Review Comments

Goal 3: Other (non-ALC)

APPLICATION OF KNOWLEDGE AND SKILLS – DIGITAL FORENSIC INVESTIGATION. Students earning a graduate degree in Cybercrime will be able to conduct a digital forensic examination in accordance with established professional protocols and demonstrate an ability to apply proper techniques and procedures to the examination of digital evidence.

1a. Student Learning Outcome Statement *Audit Review: AC*

Students will be able to identify and explain common operating systems, file structures of each, and digital artifacts associated with each as well as describe categories of digital evidence found on digital devices and identify specific types within each category.

1b. Method of Assessment *Audit Review: AC*

Cybercrime faculty have developed a large test bank of multiple choice and true/false questions that address the students' comprehension and understanding of key concepts and applications. Questions randomly drawn from the test bank are administered to CJE6626 students at 2 times during the 8-week term in which they take the course. The percentage of correct responses on each of the questions will be determined. Analysis of the results and their trend over time will help assess student performance and guide the development of future course materials.

1c. Performance Targets *Audit Review: AC*

Success will be demonstrated by at least 70% of the students scoring 80% correct responses or better on each of the two assessments in CJE 6626.

1d. Assessment Results *Audit Review: AC*

The following results are for the Summer 2019 term of CJE 6626:

Summer 2019	N	High Score	Low Score	Average	# Above 80%	% Above 80

Quiz 1	18	97	53	82	13	72%
Quiz 2	18	100	53	81	10	56%

Performance targets were not met on Quiz #2.

1e. Use of Assessment Results *Audit Review: AC*

CJE6626 is primarily a laboratory-based course that covers a wide range of applied topics. The concepts assessed on the exams relate directly to the hands-on exercises completed by the students. The Summer 2019 term run of this course was the first time it had been used in the CyberCRIME program, although it has been used very successfully in the CyberSECURITY program for the past five years.

By comparison, an identical version of this course was run at the same time for the CyberSECURITY students. The results are quite different:

CyberSECURITY students, CJE 6626, Summer 2019

Summer 2019	N	High Score	Low Score	Average	# Above 80	% Above 80
Quiz 1	12	97	73	88	11	92%
Quiz 2	12	97	67	85	9	75%

There appears to be a difference between the two groups of students likely based on their backgrounds coming into their respective programs. The CyberSECURITY students come from backgrounds characterized by prior experience and/or formal training in computer science fields. The CyberCRIME students come from a variety of backgrounds, but primarily in the social sciences, which may indicate a need to more specifically adjust the lectures and exercises to account for the lack of previous technical experience or knowledge brought into the program by the CyberCRIME students.

Course topics associated with lower performance items will receive additional attention in the development of course material revisions and future teaching strategies.

Plan Review Comments

Report Review Comments

2a. Student Learning Outcome Statement *Audit Review: AC*

Students will demonstrate the ability to apply digital forensic software tools in the processing and analysis of digital media.

2b. Method of Assessment *Audit Review: AC*

Cybercrime faculty have developed two fill-in-the blank and discussion examinations that assess the student's ability to apply knowledge and skill to the processing and analysis of a piece of digital media. Analysis of the results and their trend over time will help assess student performance and guide the development of future course materials.

2c. Performance Targets *Audit Review: AC*

Success will be demonstrated by at least 70% of the students scoring 80% correct responses or better on each of the two applied assessments.

2d. Assessment Results *Audit Review: AC*

The following results are for the Summer 2019 term of CJE 6626:

Summer 2019	N	High Score	Low Score	Average	# Above 80%	% Above 80
Quiz 1	18	100	64	81	10	56%
Quiz 2	18	100	43	88	14	78%

Performance targets were not met on Quiz #1.

2e. Use of Assessment Results *Audit Review: AC*

CJE6626 is primarily a laboratory-based course that covers a wide range of applied topics. The concepts assessed on the exams relate directly to the hands-on exercises completed by the students. The Summer 2019 term run of this course was the first time it had been used in the CyberCRIME program, although it has been used very successfully in the CyberSECURITY program for the past five years.

By comparison, an identical version of this course was run at the same time for the CyberSECURITY students. The results are quite different:

CyberSECURITY students, CJE 6626, Summer 2019

Summer						

2019	N	High Score	Low Score	Average	# Above 80	% Above 80
Quiz 1	12	100	84	96	12	100%
Quiz 2	12	100	79	95	11	92%

There appears to be a difference between the two groups of students likely based on their backgrounds coming into their respective programs. The CyberSECURITY students come from backgrounds characterized by prior experience and/or formal training in computer science fields. The CyberCRIME students come from a variety of backgrounds, but primarily in the social sciences, which may indicate a need to more specifically adjust the lectures and exercises to account for the lack of previous technical experience or knowledge brought into the program by the CyberCRIME students.

Course topics associated with lower performance items will receive additional attention in the development of course material revisions and future teaching strategies.

Plan Review Comments

Report Review Comments

Assessment Methods

Course Related Assessments

Cumulative Assessments

Performance Related Assessments

External-course Assessments

Standard Assessments