Information Technology and Management Assessment Plan for Graduate Degrees, 2019-2021 (Version 3)

Assessment plans for 2019-2021 will adhere to the rubric as defined by the IIT Assessment Report Evaluation Rubric. One Program Educational Objective (PEO) in each degree program will be assessed each term, and all objectives will be assessed twice in each three-year cycle. The full list of Program Educational Objectives to be assessed follows beginning on page 3 below. In addition to the Program Educational Objective, course objectives for each course will be assessed. Separate plans will be used for the undergraduate and graduate programs. This document addresses the courses in the Graduate Program. It was revised in Fall 2019 to reflect inclusion of the Master of Science in Information Technology and Management (MSITM), but assessment of this degree will not begin until Fall 2021 when the first students in this degree are expected to matriculate. It was revised again in Spring 2020 to reflect personnel changes and changed course offerings by semester.

Spring 2019:

Master of Information Technology and Management (MITM) PEO Assessed: 3
Master of Cyber Forensics and Security (MCYF) and M.S. in Applied Cybersecurity and Digital Forensics (MSACDF) PEO Assessed: 2
M.S. in Applied Cybersecurity and Digital Forensics (MSACDF) PEO Assessed: 4
Student Artifacts: Survey / April 2019 / Evaluation by ITM Curriculum Committee members
Assignments / May 2019/ Evaluator(s) TBD
Courses assessed:

Curricular Area	*Course*
Software Development (MITM)	ITMD 510 Object-Oriented Application Development
Security & Forensics (MCYF)	ITMS 583 Digital Evidence
Security Technologies (MSACDF)	ITMS 549 Cyber Security Technologies: Projects & Advanced Methods

Fall 2019:

Master of Information Technology and Management PEO Assessed: 1
Master of Cyber Forensics and Security and M.S. in Applied Cybersecurity and Digital Forensics PEO Assessed: 3
Student Artifacts: Survey / November 2019 / Evaluation by ITM Curriculum Committee
Assignments / December 2019 / Evaluators: Evaluator(s) TBD
Courses assessed:

Curricular Area	*Course*
System Technologies (MITM)	ITMO 540 Introduction to Data Networks & the Internet
Security Technologies (MCYF and MSACDF)	ITMS 548 Cyber Security Technologies

Spring 2020:

Master of Information Technology and Management PEO Assessed: 2
Master of Cyber Forensics and Security and M.S. in Applied Cybersecurity and Digital Forensics PEO Assessed: 2

Spring 2020 (continued):

Student Artifacts: Survey / April 2020 / Evaluation by ITM Curriculum Committee
Assignments / May 2020 / Evaluator(s) TBD

Courses assessed:

Curricular Area	Course
I.T. Infrastructures (MITM)	ITMO 554 Operating Systems Virtualization
Security Technologies (MCYF and MSACDF)	ITMS 538 Digital Forensics

Fall 2020:

Master of Information Technology and Management PEO Assessed: 1

Master of Cyber Forensics and Security and M.S. in Applied Cybersecurity and Digital Forensics PEO: 1

M.S. in Applied Cybersecurity and Digital Forensics PEO Assessed: 4

Student Artifacts: Survey / November 2020 / Evaluation by ITM Curriculum Committee
Assignments / December 2020 / Evaluator(s) TBD

Courses assessed:

Curricular Area	Course
Data Management (MITM)	ITMD 527 Data Analytics
Security Management (MCYF and MSACDF)	ITMS 578 Cyber Security Management
Thesis Research (MSACDF and MSITM)	ITMT 591 Independent Study and Research

Spring 2021:

Master of Information Technology and Management and Master of Science in Information Technology and Management PEO Assessed: 3

Master of Cyber Forensics and Security and M.S. in Applied Cybersecurity and Digital Forensics PEO Assessed: 3

Student Artifacts: Survey / April 2021 / Evaluation by ITM Curriculum Committee
Assignments / May 2021 / Evaluator(s) TBD

Courses assessed:

Curricular Area	Course
Web Design/Development (MITM)	ITMD 565 Rich Internet Applications
Security Technologies (MCYF and MSACDF)	ITMS 548 Cyber Security Technologies

Fall 2021:

Master of Information Technology and Management and Master of Science in Information Technology and Management PEO Assessed: 2

Master of Cyber Forensics and Security (MCYF) and M.S. in Applied Cybersecurity and Digital Forensics PEO Assessed: 1

Student Artifacts: Survey / November 2021 / Evaluation by ITM Curriculum Committee
Assignments / December 2021 / Evaluator(s) TBD

Courses assessed:

Curricular Area	Course
I.T. Management (MITM and MSITM)	ITMM 571 Project Management for ITM
Security Technologies (MCYF and MSACDF)	ITMS 543 Vulnerability Analysis and Control

Program Education Objectives

The following program education objectives will be assessed for HLC accreditation purposes:

Master of Information Technology and Management (MITM) Program Educational Objectives
At the conclusion of their studies, graduates of the Master of Information Technology and Management should be able to:
1. Deliver optimal technical and policy technology solutions for the problems of business, industry, government, non-profit organizations, and individuals in each student's particular area of focus.
2. Work with, lead, and manage teams in an enterprise environment to collaboratively arrive at optimal technology solutions.
3. Manage and deploy information resources applicable to each student's particular area of focus in an enterprise setting.

Master of Cyber Forensics and Security (MCYF) Program Educational Objectives
At the conclusion of their studies, graduates of the Master of Cyber Forensics and Security degree should be able to:
1. Design and implement a comprehensive enterprise security program using both policy and technology to implement technical, operational, and managerial controls.
2. Comprehensively investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law.
3. Technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.

Master of Science in Applied Cybersecurity and Digital Forensics (MSACDF) Program Educational Objectives
At the conclusion of their studies, graduates of the Master of Science in Applied Cybersecurity and Digital Forensics degree should be able to:
1. Design and implement a comprehensive enterprise security program using both policy and technology to implement technical, operational, and managerial controls.
2. Comprehensively investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law.
3. Technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.
4. Conduct and report on significant research in the areas of cybersecurity and/or digital forensics.

Master of Science in Information Technology and Management (MITM) **Program Educational Objectives**
At the conclusion of their studies, graduates of the Master of Science in Information Technology and Management should be able to:
1. Deliver optimal technical and policy technology solutions for the problems of business, industry, government, non-profit organizations, and individuals in each student's particular area of focus.
2. Work with, lead, and manage teams in an enterprise environment to collaboratively arrive at optimal technology solutions.
3. Manage and deploy information resources applicable to each student's particular area of focus in an enterprise setting.
4. Apply mathematics and technical skills to research and innovation in the field.

Survey drafting and data collection staff:
    Kayla Botica, ITM Department Manager
    Ryan Nelson, ITM Director of Student Services

Assessment Evaluators:
ITM Curriculum Committee
Faculty members of the Curriculum Committee evaluate Survey Artifacts and make recommendations based on evaluations of all assessment artifacts. All full-time faculty members are voting members of the committee should they elect to participate.

    Chair: Ray Trygstad, ITM Associate Chair and Industry Professor
    Members: Jeremy Hajek, Industry Associate Professor
                  Maurice E. Dawson, Director of the Center for Cyber Security and Forensics Education and Assistant Professor
                  Louis F. McHugh IV, SAT Director of IT and Adjunct Industry Professor
                  Thomas "T.J." Johnson, Adjunct Industry Professor
                  Phillip Matuszak, Adjunct Industry Associate Professor
    Faculty: C. Robert Carlson, ITM Chair and Professor
                  Karl Stolley, Associate Professor (joint appointment)
                  Adarsh Arora, Coleman Entrepreneur-in-Residence and Industry Professor
                  James Pappademas, Industry Professor
                  Yong Zheng, Assistant Professor

All full-time faculty members may be appointed as assessment evaluators for Assignment Artifacts. Appointments will be made at the beginning of each term in which assignments will be assessed, and will assigned in the Assessment Plan for that semester.