Information Technology and Management Assessment Plan Fall 2021

Undergraduate Assessment, Fall 2021:
Based on *Information Technology and Management Assessment Plan for Undergraduate Degrees, 2019-2021 (Version 3)* http://www.itm.iit.edu/faculty/2019-2021ITMUndergraduateAssessmentPlanV3.pdf

Program Educational Objectives Assessed: 2, 4

Student Outcomes Assessed: (b), (d), (h)

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

Courses assessed:

Curricular Area	***Course***
System Integration, Local and Global Impacts of Computing	ITM 100 Intro to Information Technology as a Profession
Networking and Communications	ITMO 340 Introduction to Data Networks & the Internet
Data, Component, Connection, & and System Security / Secure Computing	ITMS 448 Cyber Security Technologies
Component & System Security	ITMS 458 Operating System Security (BSACIT only)

The following program education objective will be evaluated:

2. Perform requirements analysis, design, and administration of secure computer and network-based systems conforming to policy and best practices, and monitor and support continuing development of relevant policy and best practices as appropriate.

The following BSACIT program education elective will be evaluated in ITMS courses:

4. Design and implement an enterprise security program using both policy and technology to implement technical, operational, and managerial controls, which will technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.

The following Student Outcomes will be evaluated in ITM 100:
ITM graduates should be able to:

(d) Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles [ABET Computing Criterion 3.4]

The following Student Outcomes will be evaluated in ITMO 340:
ITM graduates should be able to:

(b) Design, implement, and evaluate a computer-based solution to meet a given set of computing requirements [ABET Computing Criterion 3.2]

The following Student Outcomes will be evaluated in ITMS 448:
BSACIT graduates should be able to:

(h) Apply security principles and practices to maintain operations in the presence of risks and threats [ABET Cybersecurity Criterion 3.6]

The following Student Outcomes will be evaluated in ITMS 458:
BSACIT graduates should be able to:

(h) Apply security principles and practices to maintain operations in the presence of risks and threats [ABET Cybersecurity Criterion 3.6]

In addition to the above, course objectives for each course will be assessed.

Graduate Assessment, Fall 2021:
Based on *Information Technology and Management Assessment Plan for Graduate Degrees, 2019-2021 (Version 3)* http://www.itm.iit.edu/faculty/2019-2021ITMGraduateProgramAssessmentPlanV3.pdf

Master of Information Technology and Management (MITM) and Master of Science in Information Technology and Management (MSITM) Program Educational Objectives Assessed: 2

Master of Cyber Forensics and Security (MCYF) and M.S. in Applied Cybersecurity and Digital Forensics (MSACDF) Program Educational Objectives Assessed: 1

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

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

The following program education objective will be evaluated in ITMM 571:
At the conclusion of their studies, graduates of the Master of Information Technology and Management and the Master of Science in Information Technology and Management should be able to:

2. Work with, lead, and manage teams in an enterprise environment to collaboratively arrive at optimal technology solutions.

The following program education objective will be evaluated in ITMS 543:
At the conclusion of their studies, graduates of the Master of Cyber Forensics and Security and the Master of Science in Applied Cybersecurity and Digital Forensics degrees 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.

Survey drafting and data collection staff:
Kayla Botica, ITM Department Manager

Assessment Evaluators:
The ITM Curriculum Committee evaluates Survey Artifacts and makes 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
Thomas "T.J." Johnson, Adjunct Industry Professor
Phillip Matuszak, Adjunct Industry Associate Professor
Faculty: Calvin Nobles, ITM Chair and Associate Professor
Karl Stolley, Associate Professor
Adarsh Arora, Coleman Entrepreneur-in-Residence and Industry Professor
James Pappademas, Industry Professor
Yong Zheng, Assistant Professor

All faculty members may be appointed as assessment evaluators for Assignment Artifacts. Student artifacts for assessment will be collected by a member of the Assessment Evaluation team and will be assessed by a range of faculty against a published rubric.