ITMS 438 RUBRIC

ITMS 438 Vulnerability Analysis and Control
Students may be scored on a scale of 1 to 5; scores of 2 and 4 may be interpolated.

Program Educational Objectives			
Objective **Score ▶**	**5**	**3**	**1**
Investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of law	The student is consistently able to investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of law	The student is generally able to investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of laws	The student is unable to investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of law
Course student outcomes Upon completion of this course the student should be able to do the following:			
Outcome **Score ▶**	**5**	**3**	**1**
Demonstrate knowledge of cyber forensic procedures, planning of analyses and the use of common tools for analysis	The student is consistently able to demonstrate knowledge of cyber forensic procedures, planning of analyses and the use of common tools for analysis	The student is often able to demonstrate knowledge of cyber forensic procedures, planning of analyses and the use of common tools for analysis	The student is unable to demonstrate knowledge of cyber forensic procedures, planning of analyses or the use of common tools for analysis
Describe several file systems including FAT, EXT, YAFFS and NTFS	The student is able to describe several file systems including FAT, EXT, YAFFS and NTFS accurately and in detail	The student is able to describe several file systems including FAT, EXT, YAFFS and NTFS with some omissions or inaccuracies	The student is unable to describe several file systems including FAT, EXT, YAFFS and NTFS
Describe several common booting procedures	The student is able to describe several common booting procedures accurately and in detail	The student is able to describe several common booting procedures with some omissions or inaccuracies	The student is unable to describe common booting procedures
Describe how to find file system objects that have been deleted or obfuscated	The student is able to describe how to find file system objects that have been deleted or obfuscated accurately and in detail	The student is able to describe how to find file system objects that have been deleted or obfuscated with some omissions or inaccuracies	The student is unable to describe how to find file system objects that have been deleted or obfuscated
Describe how to track past computer and Internet activity and to establish timelines for this activity	The student is able to describe how to track past computer and Internet activity and to establish timelines for this activity accurately and in detail	The student is able to describe how to track past computer and Internet activity and to establish timelines for this activity with some omissions or inaccuracies	The student is unable to describe how to track past computer and Internet activity and to establish timelines for this activity
Demonstrate the ability to use tools such as WinHex, EnCase, SleuthKit and Autopsy	The student has clearly demonstrated their ability to use tools such as WinHex, EnCase, SleuthKit and Autopsy	The student has demonstrated to some extent their ability to use tools such as WinHex, EnCase, SleuthKit and Autopsy	The student is unable to use tools such as WinHex, EnCase, SleuthKit and Autopsy
Demonstrate the ability to use several forensic imaging, carving and discovery tools	The student has clearly demonstrated their ability to use several forensic imaging, carving and discovery tools	The student has demonstrated to some extent their ability to use several forensic imaging, carving and discovery tools	The student is unable to use forensic imaging, carving and discovery tools
Apply security principles and practices to maintain operations in the presence of risks and threats	The student has clearly demonstrated their ability to apply security principles and practices to maintain operations in the presence of risks and threats	The student has demonstrated to some extent their ability to apply security principles and practices to maintain operations in the presence of risks and threats	The student is unable to demonstrate an ability to apply security principles and practices to maintain operations in the presence of risks and threats