St. Thomas University School of Law
Cybersecurity LL.M.
Performance Criteria and Learning Outcomes
Approved by the Faculty March 30, 2021

Students demonstrate that they have achieved these outcomes by meeting the following indicators or criteria:

Learning Outcome 1: Students will demonstrate knowledge and understanding of the policies and stakeholders involved in the internet governance debate and the technical, social, financial, and legal impact of cybercrime, cyberwarfare, and cyberpower on global commerce.
Students will demonstrate achievement of this learning outcome by …

- Criterion 1: Identifying, describing, and interpreting terms, rules, and principles of foundational and core areas of cybersecurity, cyber law, and cyber policy.
- Criterion 2: Describing the policies and stakeholders in the internet governance debate and understanding the personal, organizational and legal/regulatory context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how cybersecurity is implemented

Learning Outcome 2: Students will be able to develop strategies for risk management.
Students will demonstrate achievement of this learning outcome by…

- Criterion 1: Identifying that information risk management is a term referring to the process of documenting what information is at risk, type and level of risk realized; and the impact of realization
- Criterion 2: Describing the attributes relating to confidentiality, possession or control, integrity, authenticity, availability, and utility, any of which can make data vulnerable to attack
- Criterion 3: Understanding what may need to be protected – and some of the reasons why that protection must occur (for example, legal and regulatory drivers, customer rights or organization objectives)

Learning Outcome 3: Students will design, develop and test policies and procedures to manage enterprise security risks.
Students will demonstrate achievement of this learning outcome by …

- Criterion 1: Identifying potential threats from external sources as well as from an "insider" or trusted party.
- Criterion 2: Performing root cause analysis.
- Criterion 3: Reporting summary of findings from vulnerability testing.

Learning Outcome 4: Students will be able to evaluate and communicate the human role in security systems with an emphasis on ethics.

Students will demonstrate achievement of this learning outcome by…

- Criterion 1: Identifying the nature and sources of moral and ethical standards.
- Criterion 2: Understanding and adopting of appropriate professional, ethical, and legal practices.
- Criterion 3: Recognizing the legal, social, ethical, and professional issues involved in the exploitation of computer technology