ContinuingEducation GPRC

CONTINUING EDUCATION

COURSE OUTLINE – Threats and Vulnerabilities Scenarios

INSTRUCTOR:	N/A	**PHONE:**	780-539-2975
OFFICE:	M105	**E-MAIL:**	ce@gprc.ab.ca

PREREQUISITE(S): None

REQUIRED TEXT/RESOURCE MATERIALS:

Course materials are included.

CALENDAR DESCRIPTION:

This course examines the process of identifying and mitigating threats and vulnerabilities in information systems. It covers common categories of threats and vulnerabilities and the resources used to detect them. This course also features a number of fictional scenarios based on threats and vulnerabilities. This course is designed for IT professionals and other adult learners who are interested in information technology security, with an eye towards handling real world scenarios.

CONTACT HOURS: 5 hours

CEUs: 0.5

PDUs: 5

DELIVERY MODE: Online self-paced

TRANSFERABILITY: N/A

GRADING CRITERIA:

Upon successful completion of the course, you will receive a Certificate of Completion.

EVALUATIONS: Learners must achieve an average test score of at least 70% to meet the minimum successful completion requirement and qualify to receive IACET CEUs.

The following list outlines the PDUs you will earn for completing this course, based on the certification you have.

Designation	Technical	Leadership	Strategic/Business	TOTAL
PMP®/PgMP®	3.5	0	1.5	5
PMI-RMP®	3.5	0	1.5	5
PMI-SP®	0	0	1.5	1.5
PMI-ACP®	3.5	0	1.5	5
PfMP®	0	0	1.5	1.5
PMI-PBA®	0	0	1.5	1.5

STUDENT RESPONSIBILITIES: Completion of any practice lessons, quizzes, assignments, or tests.

COURSE SCHEDULE/TENTATIVE TIMELINE:
Dates vary (refer to website for current availability).

LEARNING OUTCOMES:
Upon successful completion of this course, learners will be able to:

- Discuss the role of governance and auditing in identifying threats and vulnerabilities
- Identify common vulnerabilities and how penetration testing and other methods can reveal them
- Explain how threats and vulnerabilities factor into risk analysis and lead to differing risk management strategies
- Describe the difference between quantitative and qualitative risk analysis
- Evaluate different security controls such as firewalls, IDS, IPS, antimalware and patch management
- Identify common threats and other attacks on networks and their hosts
- Respond appropriately to threats and vulnerabilities raised in real-world scenarios