ContinuingEducation GPRC

CONTINUING EDUCATION

COURSE OUTLINE – Access Control and Identity Management Scenarios

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

PREREQUISITE(S): Although not necessary, some foundation in IT concepts is helpful in taking this course.

REQUIRED TEXT/RESOURCE MATERIALS:

Course materials are included.

CALENDAR DESCRIPTION:

Access control is the restriction of access to a computer system. So how does a cybersecurity professional manage this access control? This course introduces the principles of access controls, beginning with the central modes of information security and continuing through various attacks and defenses. It provides an overview of Identity Management and the resources used on modern-day information systems, including Web and cloud-based ones. This course also features a number of fictional scenarios based on access control and identity management that professionals face in the real-world.

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®	4	1	0	5
PMI-RMP®	4	1	0	5
PMI-SP®	0	1	0	1
PMI-ACP®	4	1	0	5
PfMP®	0	1	0	1
PMI-PBA®	0	1	0	1

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:

- Identify the four types of information access controls
- Describe different identification methods and technologies
- Discuss different components of Authentication, Authorization and Accounting
- Describe common access control models and mechanisms
- Explain the technologies used in single-sign-on systems
- Identify common access control attacks and countermeasures
- Provide appropriate guidance in response to real-world scenarios describing Access Control and Identity management challenges