CYBR-202 – Risk Management and Threat Modelling

Technology

Effective Term & Year: Fall 2027
Course Outline Review Date: 2032-03-01

Program Area: Information Technology

Description:

Students develop practical skills in cybersecurity risk management and threat modelling to support secure system design and organizational resilience. Students apply risk management frameworks to assess and communicate risk using qualitative and quantitative methods, while developing asset inventories and threat profiles that reflect system dependencies. Emphasis is placed on identifying and analyzing technical, physical, and procedural vulnerabilities, and integrating findings into comprehensive risk assessments. Students apply threat modelling methodologies to identify and visualize threats and plan structured threat modelling activities within defined system contexts. The course also explores the integration of security-by-design principles into the software development life cycle (SDLC). Students evaluate risk treatment strategies, implement appropriate controls, and monitor risk using key risk indicators (KRIs) to support continuous improvement.

Program Information:

This course is required for the Second Year of the Cybersecurity Operations program.

Delivery Methods: Hybrid – On-campus (Face-to-Face) and Online

Credit Type: College of the Rockies Credits

Credits: 3

Instructional Activity and Hours:

Activity	Hours
Classroom, Directed Studies or Online Instruction	30
Seminar/Tutorials	
Laboratory/Studio	30
Practicum/Field Experience	
Co-op/Work Experience	
Other	
Total	60

Course Requisites:

Prior Learning and Recognition: Yes

Students are able to request formal recognition of their prior learning or experience outside the classroom. Challenge examination, portfolio-assisted assessment, work-based assessment or a combination of assessments that is appropriate to identify, assess, and recognize prior skills, competencies, and knowledge to achieve course credit. Tuition fees apply, refer to Policy 2.5.5 Prior Learning Assessment and Recognition (PLAR) or contact an education advisor for more information.

Course Transfer Credit:

For information about receiving transfer credit for courses taken at either British Columbia or Alberta institutions, please see https://www.bctransferguide.ca/ or https://transferalberta.alberta.ca . For more transfer credit information, please visit https://www.cotr.bc.ca/Transfer

All requests for course transfer credit from institutions in British Columbia or elsewhere should go to the College of the Rockies Enrollment Service office.

Textbook Resources:

Textbook selection varies by instructor and may change from year to year. At the Course Outline Effective Date the following textbooks were in use:

Please see the instructor's syllabus or check COTR's online text calculator https://textbook.cotr.bc.ca/ for a complete list of the currently required textbooks.

Learning Outcomes:

Upon the successful completion of this course, students will be able to:

- apply risk management frameworks to assess and communicate organizational cybersecurity risk using qualitative and quantitative methods, recognizing roles, responsibilities, and risk tolerance;
- develop and maintain asset inventories and threat profiles that reflect system dependencies and support proactive cybersecurity risk management;
- assess technical, physical, and procedural vulnerabilities using appropriate tools and techniques, and analyze vulnerability reports to determine exploitability;
- conduct comprehensive risk assessments by integrating vulnerability findings and applying qualitative and quantitative techniques to inform decision-making and stakeholder communication;
- apply threat modelling methodologies to identify, analyze, and visualize threats using techniques such as attack trees and attack graphs, selecting appropriate models based on context;
- plan and facilitate threat modelling activities, including defining system scope, identifying stakeholders, mapping data flows, and documenting threats, assumptions, and attack scenarios;
- integrate threat modelling and security-by-design principles into the software development life cycle (SDLC), including identifying threats during requirements and design phases; and
- evaluate and implement risk treatment and monitoring strategies, including selecting security controls, establishing key risk indicators (KRIs), and continuously improving risk management practices through review and adaptation.

Course Topics:

- Foundations of Risk Management
- Asset Identification and Valuation
- Threat Identification and Analysis
- Vulnerability Assessment and Analysis
- Threat Modelling Methodologies
- Conducting Threat Modelling
- Risk Assessment and Analysis
- Risk Treatment and Mitigation Strategies
- Integrating Threat Modelling into the SDLC (Software Development Life Cycle)
- Risk Monitoring, Review, and Improvement

See instructor’s syllabus for the detailed outline of weekly readings, activities and assignments.

Evaluation and Assessments

Assessment Type: On-Campus (face-to-face) and Online, or Hybrid

Assessment Type	% of Total Grade
Assignments	40%
Midterm	20%
In-progress	10%
Final Project	30%
Total	100%

Grade Scheme

A+	A	A-	B+	B	B-	C+	C	C-	D	F
>=90	89-85	84-80	79-76	75-72	71-68	67-64	63-60	59-55	54-50	<50

Evaluation Notes: A grade of “D” grants credit, but may not be sufficient as a prerequisite for sequential courses.

Evaluation Notes Comments:

Please see the instructor’s syllabus for specific classroom policies related to this course, such as details of evaluation, penalties for late assignments and use of electronic aids.

Exam Attendance:

Students must attend all scheduled exams at the appointed time and place. Instructors may approve an alternate exam to accommodate an illness or personal crisis. Department heads will consider other written requests. Any student who misses a scheduled exam without prior approval will receive a “0” on the exam.

Academic Policies:

College of the Rockies policies related to courses can be found at https://cotr.bc.ca/about-us/college-policies/ and include the following:

- Policy 2.1.4 Course Audit
- Policy 2.4.1 Credential Framework
- Policy 2.4.3 Students with Documented Disabilities
- Policy 2.4.4 Student Rights, Responsibilities and Conduct
- Policy 2.4.8 Academic Performance
- Policy 2.4.9 Student Feedback and Concerns
- Policy 2.4.11 Storage of Academic Works
- Policy 2.5.3 Student Appeal
- Policy 2.5.5 Prior Learning Assessment and Recognition (PLAR)

Course Changes:

The College of the Rockies updates course outlines regularly to meet changing educational, employment and marketing needs. The instructor will notify students in writing of any updates to this outline during the semester. The instructor reserves the right to revise, add or delete material while meeting the learning outcomes of this course outline.