Subject:	CIS
Course Number:	158
Descriptive Title:	Introduction to Development, Security, and Operations
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	In this course, students develop the skills necessary to provision, operate, and manage highly-available, scalable, and self-healing distributed systems in the cloud. Students also use continuous integration and development pipelines (CI/CD) to manage service delivery systems. Students learn how to deploy and automate security controls, governance and compliance, and operational processes. Finally, students build systems to define and deploy monitoring, metrics, and logging systems within the same pipelines. This class builds upon the knowledge gained with the existing cloud curriculum offered.
Prerequisite:	CIS 150
Co-requisite:	
Recommended Preparation:	CIS 13
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	3
Outside Study Hours:	4
Total Course Hours:	90
Course Units:	3
Grading Method:	Letter Grade only
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	
Transfer UC:	Yes
Effective Date:	
General Education ECC:	
Term:	
Other:	
CSU GE:	
Term:	
Other:	
IGETC:	
Term:	

Other:	
CalGETC:	
Term:	
Other:	
Student Learning Outcomes:	At the end of this course, students will be able to: 1. Build an automated cloud infrastructure deployment including operating systems and advanced networking and routing techniques. 2. Understand and develop competency in modern development, security, and operations processes and methodologies. 3. Understand and troubleshoot full-stack deployments including database querying and application code.
Course Objectives:	1. Implement and automate testing for a continuous development and integration pipeline (CI/CD). 2. Implement deployment strategies for various server technologies such as containers and instances. 3. Define cloud infrastructure and other components using platform-agnostic tools to provision and manage systems. 4. Design and build automated solutions for complex enterprise deployments. 5. Implement high-availability and scalable solutions to meet required resilience metrics. 6. Implement automated recovery processes to meet RTO and RPO objectives. 7. Configure, automate, audit, analyze and store a large volume of logs and metrics from disparate systems. 8. Configure and manage event sources to process, notify, and automate responses to specific events. 9. Implement identity and access management at scale. 10. Implement automation for security monitoring, controls, auditing, and data protection. 11. Troubleshoot a wide variety of system errors and failures.
Major Topics:	1. Software Development Lifecycle Automation (6 hours, Lecture) A. CI/CD Pipelines B. Automated testing into CI/CD pipelines C. Deployment strategies for various server technologies 2. Configuration Management and Infrastructure as Code (6 hours, Lecture) A. Enterprise infrastructure and reusable components B. Automated solutions for complex tasks and enterprise scale environments 3. Resilient Cloud Solutions (6 hours, Lecture) A. High-availabiility solutions B. Scalable solutions C. Automated recovery 4. Monitoring and Logging (6 hours, Lecture) A. Collecting, storing, aggregating logs and metrics. B. Audit, monitor, and analyze logs and metrics C. Automated monitoring and event management 5. Incident and Event Response (6 hours, Lecture) A. Event sources B. Responding to events

	C. Troubleshooting system failures and errors 6. Security and Compliance (6 hours, Lecture) A. Identity and Access Management B. Automated security controls and data protection C. Automated security monitoring and auditing 7. Software Development Lifecycle Automation (6 hours, Lab) A. CI/CD Pipeline Tools and Usage B. Automated Testing Into CI/CD pipelines 8. Configuration Management and Infrastructure as Code (10 hours, Lab) A. Configuring Enterprise Infrastructure B. Writing Code to Deploy Resources C. Automating Solutions for Complex Tasks 9. Resilient Cloud Solutions (10 hours, Lab) A. Exploring High-availability Solutions B. Exploring Scalability Solutions C. Integrating Automated Recovery 10. Monitoring and Logging (8 hours, Lab) A. Collecting, Storing, & Aggregating Logs and Metrics B. Audit, Monitor, and Analyze Logs and Metrics C. Automated Monitoring and Event Management 11. Incident and Event Response (8 hours, Lab) A. Identifying and Configuring Event Sources B. Automating Responding to Events C. Troubleshooting System Failures and Errors 12. Security and Compliance (12 hours, Lab) A. Identity and Access Management Configuration B. Automated Security Controls and Data Protection C. Automated Security Monitoring and Auditing
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
A.1. Primary Methods of Evaluation (Part 1 - CCN courses only):	
Primary Method of Evaluation:	2) Problem solving demonstrations (computational or non-computational)
Typical Assignment Using Primary Method of Evaluation:	Configure monitoring and logging for your CI/CD pipeline using cloud services. Set up alarms and notifications for critical events or failures in your pipeline. Document your implementation in a 1-2 page report including screenshots and configuration parameters.
Critical Thinking Assignment 1:	Analyze and design a CI/CD pipeline using platform-agnostic tools. Explore different strategies and their contributions to resilience. Design the pipeline after selecting the most appropriate strategy. Implement your pipeline while documenting all steps involved. Analyze the implementation and performance of your pipeline using metric-measurement tools. Document all the steps involved and present your implementation to the class.
Critical Thinking Assignment 2:	Explore and implement a cloud deployment using Infrastructure as Code practices.

	Explore different configuration management strategies and options available to deploy services using IaC (Infrastructure as Code). Evaluate each service including how it can be used, considering factors like flexibility, scalability, security, and compliance. Design and deploy the multi-architecture deployment. Document and present all steps involved to the class.
Other Evaluation Methods:	Class Performance, Laboratory Reports, Performance Exams, Quizzes
If Other:	
Instructional Methods:	Demonstration, Lab, Lecture, Multimedia presentations
If other:	
Work Outside of Class:	Answer questions, Problem solving activity, Required reading, Skill practice, Written work (such as essay/composition/report/analysis/research)
If Other:	
Up-To-Date Representative Texts:	RIBEIRO, M. (2022). Learning DEVSECOPS: Integrating continuous security across your organization. O'REILLY MEDIA.
Alternative Texts:	
Required Supplementary Readings:	
Other Required Materials:	
Requisite	Prerequisite
Category	sequential
Requisite course:	CIS 150 - Cloud Computing with AWS
Requisite and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s).	**Student must be able to create a cloud application utilizing AWS Computing Services (EC2)** CIS 150: Create a cloud application utilizing AWS Computing Services (EC2)
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill(s). if applicable	
Requisite course:	CIS 13
Requisite and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s).	**Student must be able to solve common business problems using appropriate information technology applications and systems.** CIS 13: Solve common business problems using appropriate information technology applications and systems.
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding	

course objective under each skill(s). if applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	Martin Anaya
Date:	10/9/2025
Original Board Approval Date:	01/21/2026
Effective Term:	FA 2026