APPLIED CYBERDEFENSE NETWORK OPERATIONS, BACHELORS OF SCIENCE

The Bachelor of Science in Applied Cyberdefense Network Operations (ACNO) prepares students for advanced roles securing, operating, and defending enterprise and cloud computing environments. Building on lower-division coursework in information technology, cybersecurity, or related fields, the program emphasizes cybersecurity operations, secure networking, cloud services and cloud security, incident response, and responsible use of artificial intelligence tools to support analysis and documentation. The curriculum combines lecture with intensive laboratory experiences aligned with industry standards and regional workforce needs.

Admission is by application through a multi-criteria selection process due to limited program capacity. Applicants are expected to demonstrate appropriate lower-division preparation, typically through completion of an Associate of Science degree in Information Technology, Cybersecurity, or a closely related discipline, or equivalent coursework. Students entering the program should possess foundational skills in networking, operating systems, and cybersecurity principles to ensure readiness for upper-division study.

The program provides a clear pathway for graduates of regional community college information technology and cybersecurity programs, minimizing duplication of coursework and supporting timely completion. Students with relevant Associate of Science degrees are strong transfer candidates.

Graduates will demonstrate the ability to implement, secure, monitor, and troubleshoot complex digital infrastructures; apply defensive cybersecurity practices; respond to security incidents; manage risks in enterprise and cloud environments; and communicate technical information effectively. The program aligns with industry-recognized certifications and prepares graduates for high-demand careers in cybersecurity, network operations, and cloud security while supporting continued professional development.

Admission to the Applied Cyberdefense Network Operations (ACNO) Bachelor's Degree

To qualify for admission into the BS in Applied Cyberdefense Network Operations program, students must have:

1. Earned an Associate degree in a related Information Technology or Cybersecurity Major. Consult with the discipline faculty if you have coursework that is not from Moorpark College.
2. Completed the California General Education Transfer Curriculum (Cal-GETC) pattern. Students with catalog rights and who have maintained continuous enrollment can continue to complete the CSU GE or IGETC.
3. Met all admission program requirements, including but not limited to the courses listed below in the Program Requirements for the Associate Degree.
4. Provided transcripts from all colleges attended.

After admission to the ACNO program, students must:

1. Complete all upper-division major coursework as designated in the Program Requirements. Each course for the major must be completed with a grade of "C" or better.
2. Complete 9 semester units of upper division general education (from two different disciplines outside of the major) as designated in the program requirements.
3. Complete the 128-136 units required for the bachelor's degree.

ACNO M301 Advanced Cisco II 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Examines the design and security of complex enterprise networks. Covers advanced routing, switching, and redundant architectures with an emphasis on applied cybersecurity. Develops student skills in securing local area networks (LANs), implementing Layer 2 defenses, configuring access control lists (ACLs), and deploying secure remote access using virtual private networks (VPNs). Explores wireless local area network (WLAN) security, network address translation (NAT), and troubleshooting techniques in modern enterprise infrastructures.
Catalog Notes: Course prepares students for the Cisco Certification Exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M302A Microsoft Hybrid Server 1 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Introduces administration of Microsoft hybrid server environments that integrate on-premises Windows Server infrastructure with Microsoft Azure services. Covers identity services, virtualization, storage, networking, security, and hybrid connectivity. Emphasizes deployment, management, and troubleshooting of enterprise server systems in hybrid cloud environments.
Catalog Notes: Prepares students for Microsoft professional certification.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M302B Microsoft Hybrid Server 2 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Prerequisites: ACNO M302A
Enrollment Limitations: Admitted to the program. Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Builds on foundational hybrid server administration skills and focuses on advanced management of Microsoft hybrid server environments integrating on-premises Windows Server with Microsoft Azure. Covers advanced identity services, networking, storage, virtualization, security, monitoring, and troubleshooting in enterprise hybrid infrastructures. Emphasizes operational reliability, performance, and secure administration of complex hybrid server environments.
Catalog Notes: Prepares students for Microsoft professional certification.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M304 Virtualization Technology 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Introduces the design, deployment, and management of enterprise virtualization technologies. Covers hypervisor architecture, virtual machines, virtual networking, storage integration, high availability, resource allocation, and operational management in data center and hybrid environments. Emphasizes platform-agnostic principles applicable across commercial and open-source technologies, supported by hands-on laboratory experience using enterprise virtualization platforms.
Catalog Notes: Prepares students for VMware or other virtualization professional certifications.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M305 AWS Cloud Foundations 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Examines foundational concepts in cloud computing. Covers core cloud terminology, shared responsibility, identity and access management fundamentals, basic networking concepts, and the purpose of key cloud services for compute, storage, and databases. Emphasizes secure configuration habits, cost awareness, and cloud governance basics. Employs guided labs to create and manage cloud resources, to review security settings, and to interpret basic monitoring outputs.
Catalog Notes: Course prepares students for an entry-level Amazon Web Services cloud certification exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M306 Azure Cloud Administrator 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Prepares students to deploy, configure, secure, and manage cloud infrastructure in Microsoft Azure environments. Instructs implementation of identity management, networking, storage, compute resources, monitoring, and governance using industry best practices. Introduces the use of cloud-native artificial intelligence services to automate operations, analyze system telemetry, enhance security monitoring, and support intelligent decision-making in enterprise environments. Emphasizes secure configuration, cost optimization, high availability, and responsible use of AI tools in cloud administration.
Catalog Notes: Course prepares students for the Microsoft Azure Administrator certification exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M307 Cloud Architecture 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Prerequisites: ACNO M305
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Provides students with an overall understanding of designing distributed applications and systems in the cloud. Includes a detailed overview of designing and deploying scalable, highly available, and fault-tolerant architectures, with attention to information assurance best practices to enhance security and support cost-aware design decisions. Reviews cloud tools and examine the responsible use of artificial intelligence features and tools that support cloud deployment, management, monitoring, and security operations.
Catalog Notes: Helps prepare students for the Amazon Web Services Solutions Architect certification exam.
Grade Modes: Letter Graded, Credit by exam, license etc., Student Option-Letter/Credit, Pass/No Pass Grading
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M308 Firewall Security 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Examines the design, configuration, and management of enterprise firewall and next-generation firewall security technologies. Covers firewall architecture, security policy design, network address translation, intrusion prevention, application-aware filtering, threat detection, and network segmentation across on-premises and cloud environments. Emphasizes secure policy implementation, operational management, and troubleshooting of enterprise firewall infrastructures using industry-standard platforms.
Catalog Notes: Course prepares students for the Palo Alto professional certification exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M401 Cloud Databases 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Prerequisites: ACNO M307
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Develops hands-on skills to select, deploy, secure, monitor, and recover cloud database workloads. Employs guided labs for designing secure network boundaries for database services, implementing encryption and key management practices, managing identities, roles, and secrets, configuring high availability and disaster recovery, and validating operational controls. Emphasizes utilization of modern cloud database management systems and database administration, with comparative coverage of additional database platforms and service models. Instructs the use of command-line tools and infrastructure-as-code practices to provision and manage database resources and apply responsible, AI-assisted workflows to support query tuning, troubleshooting, and implementing best practices to security attainment.
Catalog Notes: Course helps prepare student to pass Amazon Web Services database certification.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M402 Certified Ethical Hacker 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Provides advanced instruction in penetration testing methodologies and authorized security assessment practices in enterprise environments. Covers structured engagement phases including reconnaissance, vulnerability assessment, exploitation testing, post-exploitation analysis, and professional reporting. Emphasizes rules of engagement, legal and ethical considerations, risk evaluation, and remediation strategies. Requires extensive laboratory activities in which students design and document penetration testing engagements in controlled environments.
Catalog Notes: Prepares students for the Certified Ethical Hacker (CEH) professional certification; EC-Council.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M403 Cisco CyberOps 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Prepares students for work in a security operations center by teaching security monitoring, host-based analysis, network intrusion analysis, and incident response workflows. Instructs students how to analyze real telemetry (logs, alerts, packet captures, and flow records), correlate events across data sources, and document findings using standard investigative methods. Incorporates hands-on labs to utilize common open-source security tools, and also virtual lab environments to simulate real-world incident detection, triage, escalation, and reporting.
Catalog Notes: Course helps prepare students for the Cisco CyberOps Certification Exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M404 Identity Protection Security 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Provides advanced instruction in identity and access management security within hybrid and cloud enterprise environments. Covers authentication protocols, multi-factor authentication, conditional access policies, privileged access management, and identity governance controls. Emphasizes zero-trust principles, policy enforcement, threat detection, and compliance requirements. Requires laboratory activities in which students configure and secure directory services and cloud-based identity platforms in controlled environments.
Catalog Notes: Course prepares students for the Microsoft professional certification exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M405 Azure Cloud Security 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Prerequisites: ACNO M306
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Prepares students to design, implement, and operate security controls in Microsoft Azure, with emphasis on identity governance, network protection, data security, security posture management, and security operations workflows. Trains students to configure and validate Azure security baselines using Microsoft Entra ID, Azure network security capabilities, data protection controls, and cloud workload protection with Microsoft Defender for Cloud. Guides students to perform cloud-native monitoring, threat hunting, and with responding to incidents using Azure security and logging tools to support detection, triage, containment, and reporting.
Catalog Notes: Course helps prepare to pass the Microsoft Azure security certification exam and helps prepare students for workforce.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M406 CompTIA Security Practitioner 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Provides advanced instruction in enterprise security architecture and secure systems engineering across hybrid, cloud, and on-premises environments. Covers integrated security solutions including cryptographic controls, network and system hardening, risk management frameworks, and incident response strategies. Emphasizes alignment of technical safeguards with organizational risk, compliance requirements, and operational resilience. Requires laboratory activities in which students evaluate, design, and deploy enterprise-level security controls in complex environments.
Catalog Notes: Course prepares students for the CompTIA SecurityX professional certification exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M407 AWS Cloud Security 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Prerequisites: ACNO M307
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Prepares students to design, implement, and operate security controls in Amazon Web Services (AWS) cloud environments, with emphasis on identity governance, network protection, data security, security posture management, and security operations workflows. Instructs students to configure and validate security baselines using AWS identity and access management, network segmentation and filtering controls, encryption and key management practices, and cloud workload protection services. Guides students to perform cloud-native monitoring, threat hunting, and with responding to incidents using AWS security services and centralized logging to support detection, triage, containment, recovery, and reporting. Requires hands-on laboratories to use a controlled AWS environment and a virtual lab setting to simulate realistic enterprise scenarios to document findings and actions using standard security practices.
Catalog Notes: Course supports workforce preparation and helps prepare students for AWS security certification exam.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M408 Device and Network Forensics 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Develops applied skills for acquiring, preserving, analyzing, and reporting digital evidence from host devices, network environments, mobile devices, and cloud platforms. Guides students with proper evidence handling, chain of custody documentation, and forensic readiness in alignment with common legal and organizational requirements. Instructs students with proper techniques in collecting and analyzing artifacts from personal computers, servers, removable media, mobile operating systems, cloud service logs, and network traffic to reconstruct events and support incident response and investigations. Requires laboratory activities emphasizing forensically sound acquisition, integrity validation using cryptographic hashes, timeline reconstruction, and evidence based conclusions.
Catalog Notes: The course develops competencies consistent with industry-recognized digital forensics certification standards, strengthening workforce readiness in forensic investigation and incident response roles.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M409 Risk Management 3 Units
In-Class Hours: 35 lecture, 52.5 laboratory
Enrollment Limitations: Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies.
Provides advanced instruction in enterprise risk management and information systems audit within cybersecurity environments. Covers quantitative and qualitative risk assessment methods, development of risk registers, evaluation of technical controls, and assessment of compliance with governance frameworks and regulatory requirements. Emphasizes information technology audit methodology, policy development, control testing, and executive-level reporting. Requires laboratory and project activities in which students conduct simulated information technology audit engagements and present risk-based recommendations aligned with organizational objectives.
Catalog Notes: Course prepares students for the Certified Information Systems Auditor professional certification exam; Information Systems Audit and Control Association.
Grade Modes: Letter Graded
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

ACNO M480 Work Experience Education in Applied Cyberdefense Network Operations Program 1-14 Units
In-Class Hours: 54-756 paid cooperative
Enrollment Limitations: - Successful admission into the Applied Cyberdefense Network Operations (ACNO) Bachelor of Science program, indicating completion of all required foundational lower-division competencies; and - Instructor approval and completion of or concurrent enrollment in one course within the work experience discipline.
Prepares students for workforce entry by providing on-the-job learning to develop effective work habits, attitudes, and career awareness in paid or unpaid work experience that are related to the discipline. Requires the development and documentation of learning objectives and the completion of a paper, presentation, and/or project. Includes both workplace supervisor and faculty adviser advisor feedback and/or written evaluations.
Catalog Notes: To take this course, contact the Career Center; requires orientation session; students receive one unit of credit for each 54 hours of unpaid or paid work; Students may enroll in up to 14 semester units of work experience education per semester or term; there is no limit to the number of terms for which a student may enroll in work experience education.
Grade Modes: Letter Graded
Repeatable for Credit: Course may be repeated up to a maximum of 14 units of credit.
Field Trips: May be required
Degree Applicability: Applies to Associate Degree
AA/AS GE: None
Transfer Credit: CSU
UC Credit Limitations: None

Course ID	Title	Units/ Hours
Lower-Division Major Requirements (AS Degree)		
CNSE M01	Networking Fundamentals	4
CNSE M06	Cisco Fundamentals of IT Essentials: PC Hardware & Software	4
CNSE M18	Cisco System Computer Networking A	4
CNSE M30	MS Windows Administration	3
CNSE M55	Linux Networking and System Administration	3
CNSE M57	Scripting for Security Management	3
CNSE M80	Work Experience Education in Computer Network Systems Engineering	1-4
CNSE M82	Introduction to Network Security	3
LIST A: Select one of the following courses (3-4 units)		
CNSE M13	Internetworking and TCP/IP	4
CNSE M19	Cisco System Computer Networking B	4
CNSE M31	MS Windows Network Server	3
LIST B: Select and complete two courses (5-6 units)		
CNSE M56	CompTIA Advanced Security Practitioner Preparation	3
CNSE M83	Introduction Computer Forensics	3
CNSE M84	Certified Ethical Hacker	2
CNSE M86	Firewall Administration	3
CNSE M100	Cybersecurity Analysis	3
CNSE M105	AWS Cloud Foundations	3
CNSE M111	Azure Cloud Fundamentals	3
CNSE M170	Cloud Security	3

Total Units for the Lower-Division Major Requirements		**33-38**
Upper-Division Major Requirements		
ACNO M301	Advanced Cisco II	3
ACNO M302A	Microsoft Hybrid Server 1	3
ACNO M302B	Microsoft Hybrid Server 2	3
ACNO M304	Virtualization Technology	3
ACNO M305	AWS Cloud Foundations	3
ACNO M306	Azure Cloud Administrator	3
ACNO M307	Cloud Architecture	3
ACNO M308	Firewall Security	3
ACNO M401	Cloud Databases	3
ACNO M402	Certified Ethical Hacker	3
ACNO M403	Cisco CyberOps	3
ACNO M404	Identity Protection Security	3
ACNO M405	Azure Cloud Security	3
ACNO M406	CompTIA Security Practitioner	3
ACNO M407	AWS Cloud Security	3
ACNO M408	Device and Network Forensics	3
ACNO M409	Risk Management	3
ACNO M480	Work Experience Education in Applied Cyberdefense Network Operations Program	1-4
Upper-Division General Education (GE)		
BUS M400	Project Management	3
ENGL M300	Technical Writing	3
PHIL M400	Ethics in the Age of Emerging Technology	3
Total Units for the Upper-Division Major and GE Requirements		**61-64**

Course ID	Title	Units/ Hours
Total Units for the Major (Lower and Upper-Division)		**94-102**
Cal-GETC Pattern		**34**
Double-Counted Units		0
Elective Units		0
Total Units for the BS Degree		**128-136**

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

- design, configure, and validate secure routed/switched networks and perimeter defenses using enterprise networking and firewall security platforms .
- deploy cloud workloads and hybrid integrations with secure networking, identity, monitoring, and resilience controls using cloud administration and cloud architecture competencies.
- secure virtualization-based environments (segmentation, hardening baselines, patch/upgrade strategy, backup/recovery validation) suitable for modern cyber labs and enterprise deployments.
- assess identity protection controls to reduce account takeover and lateral movement risk in cloud/hybrid environments.
- plan and execute ethical hacking workflows (recon, vulnerability validation, exploitation in controlled conditions) and deliver professional findings and prioritized mitigations.
- triage and investigate security events, apply automation/scripting and AI-assisted analytics to improve detection/response speed and consistency, perform device/network forensics, and communicate results through professional writing, project execution, and internship-based practice.
- implement robust security controls and risk-mitigation frameworks, ensuring all project lifecycles are built upon a foundation of proactive defense and resilience.