COURSE SYLLABUS

Zero Trust & Modern Access Certificate Program

A three-course live path through identity and phishing-resistant MFA, zero trust architecture implementation, and the FedRAMP transition from Rev5 to 20x and CR26.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/certificates/zero-trust-and-modern-access-certificate-program

support@graduateschool.edu •
(888) 744-4723

Course Outline

This package includes these courses

- ICAM and MFA Fundamentals Course (6.5 Hours)
- Zero Trust Architecture Implementation (10 Hours)
- FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26 (12 Hours)

ICAM and MFA Fundamentals Course

A foundational pass through Identity, Credential, and Access Management for federal staff, running the full chain from identity through proofing, authentication and MFA, authorization, and federation to the access decision.

- Identity, account, credential, and authenticator distinguished, and how authentication, authorization, and access relate
- Identity proofing and the joiner, mover, and leaver lifecycle
- The assurance-level model — IAL, AAL, and FAL — applied to real access situations
- Common MFA methods compared, and why stronger methods carry greater assurance
- Attacks aimed at MFA: phishing, MFA fatigue, credential theft, and adversary-in-the-middle
- Least privilege, need-to-know, RBAC, and ABAC in authorization decisions
- Federation and single sign-on, including identity providers, relying parties, and assertions
- A full access transaction worked end to end

Zero Trust Architecture Implementation

An intermediate course taking zero trust from principle to a staged, governed implementation plan.

- Zero trust principles and the federal drivers behind them
- Current-state maturity assessment using the CISA ZT Maturity Model
- Identity, credential and access management modernization

- Trust enforcement across devices, networks and workloads
- Application, data and policy enforcement architecture
- Visibility, analytics and automation for threat response
- A staged zero trust implementation roadmap

FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26

Get clear on what FedRAMP's shift to 20x and the Consolidated Rules for 2026 actually change, and leave with a transition roadmap. Timed to the January 1, 2027 CR26 deadline.

- Explain CR26 and the FedRAMP modernization timeline running through 2028
- Set Rev5 authorization against 20x certification
- Describe the new certification classes and what changes about boundaries
- Modernize packages around Security Decision Records and structured data
- Put Key Security Indicators and automated validation to work
- Draft a Rev5-to-20x transition roadmap