COURSE SYLLABUS

Zero Trust & Modern Access Certificate Program (Self-Paced)

A four-course self-paced path covering cryptography essentials, identity and phishing-resistant MFA, zero trust architecture implementation, and the FedRAMP move from Rev5 to 20x and CR26.

> Group classes (Live Online) and onsite training are 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-self-paced



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

Course Outline

This package includes these courses

- Cryptography Essentials Course (Self-Paced) (12 Hours)
- ICAM and MFA Fundamentals Course (Self-Paced) (6 Hours)
- Zero Trust Architecture Implementation (Self-Paced) (12 Hours)
- FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26 (Self-Paced) (12 Hours)

Cryptography Essentials Course (Self-Paced)

Learn how encryption, hashing, and digital signatures work and where each fits, so you can make sound cryptography decisions.

- Explain the four core goals cryptography provides: confidentiality, integrity, authenticity, and non-repudiation.
- Distinguish symmetric encryption from asymmetric encryption and explain when each is used.
- Explain how a public and private key pair solves the key distribution problem.
- Use a hash value to verify that a file or message has not been altered.
- Explain why passwords are hashed rather than encrypted.
- Describe how a digital signature is created and verified, and why it provides non-repudiation.
- Explain what public key infrastructure solves and how a certificate authority establishes trust.
- Interpret the fields in a digital certificate and explain what certificate revocation means.
- Explain how TLS protects data in transit and why HTTPS depends on it.
- Distinguish encryption at rest from encryption in transit and identify where each applies.
- Describe, at a conceptual level, how a virtual private network protects traffic.
- Identify weak or outdated cryptographic algorithms and explain why they remain a risk.
- Recognize how poor key management can defeat otherwise strong encryption.

ICAM and MFA Fundamentals Course (Self-Paced)

Foundational Identity, Credential, and Access Management for federal staff, covering the chain from identity and proofing through authentication, MFA, authorization, and federation to the access decision.

- Identity, account, credential, and authenticator, and how authentication, authorization, and access relate
- Identity proofing and the joiner, mover, leaver lifecycle
- IAL, AAL, and FAL applied to real access situations
- Common MFA methods compared by assurance
- MFA-targeted attacks: phishing, MFA fatigue, credential theft, adversary-in-the-middle
- Least privilege, need-to-know, RBAC, and ABAC in authorization
- Federation and single sign-on: identity providers, relying parties, assertions
- An end-to-end access transaction and access decision

Zero Trust Architecture Implementation (Self-Paced)

- Explain zero trust principles and the federal drivers behind them
- Assess current-state maturity using the CISA ZT Maturity Model
- Modernize identity, credential, and access management
- Enforce trust across devices, networks, and workloads
- Architect application, data, and policy enforcement
- Apply visibility, analytics, and automation for threat response
- Build a staged zero trust implementation roadmap

FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26 (Self-Paced)

Understand what FedRAMP's move to 20x and the Consolidated Rules for 2026 change, and build a transition roadmap. Timed to the January 1, 2027 CR26 deadline.

- Explain CR26 and the FedRAMP modernization timeline through 2028
- Contrast Rev5 authorization with 20x certification
- Describe the new certification classes and boundary changes
- Modernize packages using Security Decision Records and structured data
- Apply Key Security Indicators and automated validation
- Build a Rev5-to-20x transition roadmap