COURSE SYLLABUS

FPM 513: IT Infrastructure and Architectural Design Course

This course prepares federal program and project managers to design and manage IT architectures that align with agency missions and modernization goals. Participants learn to apply enterprise architecture principles, integrate cybersecurity frameworks, and develop secure, scalable, and compliant IT solutions that drive mission performance.

> 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/courses/fpm-513-it-infrastructure-and-architectural-design-course

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

Course Outline

Module 1: Introduction to IT Infrastructure and Architectural Design

- Recognize the role of IT architecture in federal project success.
- Understand OMB regulations and guidance shaping federal IT systems.
- Identify common architectures and infrastructure components across agencies.
- Outline key themes such as enterprise architecture, security, and infrastructure.

Module 2: Enterprise Architecture

- Define principles of enterprise architecture (EA) and mission alignment.
- Apply federal EA frameworks to guide agency IT planning.
- Develop baseline and target architecture models to map current and future states.
- Use EA to inform IT investment and technology roadmap decisions.

Module 3: Information Technology Architecture

- Apply architectural methods to design scalable, maintainable IT systems.
- Define modular, layered, and interoperable system design principles.
- Ensure integration with existing enterprise systems through standard interfaces.
- Document system architecture with diagrams and models for communication.

Module 4: Infrastructure Design

- Describe infrastructure components—hardware, software, networks, and telecoms.
- Understand LAN/WAN designs, communication protocols, and standards.
- Design infrastructure for performance, redundancy, and resiliency.
- Select technologies that align with enterprise needs and architecture.

Module 5: Information Assurance

- Apply security principles to protect IT systems and data (CIA triad).
- Implement access controls, authentication, and identity management.
- Use encryption, backup, and recovery to safeguard data.
- Comply with FISMA, NIST, and other federal security standards.

Module 6: Information Systems and Network Security

- Identify and mitigate vulnerabilities in systems and networks.
- Develop security plans and standard operating procedures.
- Use tools like firewalls, IDS/IPS, and encryption for layered defense.
- Establish incident response and continuity plans for security resilience.

Module 7: Information Systems Security Certification

- Apply certification and accreditation methods for system security evaluation.
- Develop test plans, control assessments, and risk documentation.
- Report findings and corrective actions for identified vulnerabilities.
- Maintain compliance through continuous monitoring post-accreditation.

Module 8: Configuration Management

- Plan and control system changes using configuration management principles.
- Establish baselines and version tracking across system lifecycles.
- Use CM tools to maintain consistency across environments.
- Ensure all changes are approved, documented, and integrity is maintained.

Module 9: IT Operations Support

- Ensure effective deployment and delivery of IT products and services.
- Oversee operations, monitoring, and help desk support to meet SLAs.
- Implement release and change management with minimal user disruption.
- Maintain service continuity through backup and failover planning.