CGRC – Governance, Risk and Compliance Certification

Course Outline

1) Prepare

- Explain the purpose and value of preparation
- Identify references associated with the Prepare step
- Identify other risk management frameworks and their relationship to RMF tasks
- Identify relevant security and privacy regulations
- List the references, processes and outcomes that define:
- Complete selected Prepare Tasks for the example system

2) Categorize

- Explain the purpose and value of categorization
- Identify references associated with the Categorize step
- List the references, processes, and outcomes that define Risk Management Framework (RMF) Task C-1: System Description
- Describe a system's architecture
- Describe an information system's purpose and functionality
- Describe and document a system's characteristics
- List the references, processes and outcomes that define RMF Task C-2: Security Categorization
- Categorize an information system
- List the references, processes and outcomes that define RMF Task C-3: Security Categorization Review and Approval
- Describe the review and approval process for security categorization
- Categorize the example systems

3) Select

- Explain the purpose and value of control selection and allocation
- Identify references associated with the Select step
- Relate the ISO 27001 Statement of Applicability to the NIST RMF
- List the references, processes and outcomes that define RMF Task S-1: Control Selection
- List the references, processes and outcomes that define RMF Task S-2: Control Tailoring
- Select appropriate security control baselines based on organizational guidance
- Tailor controls for a system within a specified operational environment
- List the references, processes and outcomes that define RMF Task S-3: Control Allocation
- List the references, processes and outcomes that define RMF Task S-4: Documentation of Planned Control Implementations
- Allocate security and privacy controls to the system and to the environment of operation
- Document the controls for the system and environment of operation in security and privacy plans
- List the references, processes and outcomes that define RMF Task S-5: Continuous

Monitoring Strategy - System

- Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy
- List the references, processes and outcomes that define RMF Task S-6: Plan Review and Approval
- Review and approve the security and privacy plans for the system and the environment of operation
- Allocate security controls for the example system
- Tailor security controls for the example system
- Draft a continuous monitoring plan for the example system

4) Implement

- Explain the purpose and value of implementation
- Identify references associated with the Implement step
- List the references, processes and outcomes that define RMF Task I-1: Control Implementation
- Identify appropriate implementation guidance for control frameworks
- Integrate privacy requirements with system implementation
- List the references, processes and outcomes that define RMF Task I-2: Update Control Implementation Information
- Update a continuous monitoring strategy
- Update a control implementation plan

5) Assess

- Explain the purpose and value of assessment
- Identify references associated with the Assess step
- Understand and identify common elements of the NIST process that are included in other frameworks and processes
- List the references, processes and outcomes that define RMF Task A-1: Assessor Selection
- List the references, processes and outcomes that define RMF Task A-2: Assessment Plan
- List the references, processes and outcomes that define RMF Task A-3: Control Assessment
- List the references, processes and outcomes that define RMF Task A-4: Assessment Reports
- List the references, processes and outcomes that define RMF Task A-5: Remediation Actions
- List the references, processes and outcomes that define RMF Task A-6: Plan of Action and Milestones
- Develop an assessment plan for identified controls in the example system
- Develop a remediation plan for unsatisfied controls in the example system

6) Authorize

- Explain the purpose and value of authorization
- Identify references associated with the Authorize step

- Relate system approvals under organizational processes to the concepts applied in the NIST RMF
- List the references, processes and outcomes that define RMF Task R-1: Authorization Package
- List the references, processes and outcomes that define RMF Task R-2: Risk Analysis and Determination
- List the references, processes and outcomes that define RMF Task R-3: Risk Response
- List the references, processes and outcomes that define RMF Task R-4: Authorization Decision
- List the references, processes and outcomes that define RMF Task R-5: Authorization Reporting
- Develop a risk determination for the example system on the system risk level
- Authorize the system for operation
- Determine appropriate elements for the Authorization decision document for the example system

7) Monitor

- Explain the purpose and value of monitoring
- Identify references associated with the Monitor step
- List the references, processes and outcomes that define RMF Task M-1: System and Environment Changes
- (Coordinate) Integrate cybersecurity risk management with organizational change management
- List the references, processes and outcomes that define RMF Task M-2: Ongoing Assessments
- Monitor risks associated with supply chain
- List the references, processes and outcomes that define RMF Task M-3: Ongoing Risk Response
- Understand elements for communication surrounding a cyber event
- List the references, processes and outcomes that define RMF Task M-4: Authorization Package Updates
- List the references, processes and outcomes that define RMF Task M-5: Security and Privacy Reporting
- List the references, processes and outcomes that define RMF Task M-6: Ongoing Authorization
- List the references, processes and outcomes that define RMF Task M-7: System Disposal
- Discuss Monitor step activities in the example system

8) CAP Certification Information