COURSE SYLLABUS

Contingency Planning and Cyber Resilience Course

Build a contingency plan that works when systems go down, from business impact analysis through recovery and testing.

> 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/courses/contingency-planning-and-cyber-resilience-course

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

Course Outline

Module 1: Foundations: Contingency Planning and Cyber Resilience

- Lessons:
  - What Contingency Planning Is, and Why It Is Not Optional
  - From Disaster Recovery to Cyber Resilience
  - A Map of Plan Types: BCP, DRP, COOP, and More
- Applied activity: Learners review a short description of an organization's disruption, a ransomware incident that takes core systems offline, and sort a list of response activities into the plan type, business continuity, disaster recovery, or incident response, each activity most naturally belongs to.

Module 2: Step 1: Contingency Planning Policy and Governance

- Lessons:
  - Why a Contingency Planning Policy Comes First
  - What a Contingency Planning Policy Should Contain
  - Roles and Responsibilities in Contingency Planning
- Applied activity: Learners review a short, incomplete policy statement and identify which required elements are missing before it could guide a real contingency planning effort.

Module 3: Step 2: Business Impact Analysis

- Lessons:
  - What a Business Impact Analysis Measures
  - Identifying Critical Systems and Processes
  - Setting Recovery Time and Recovery Point Objectives
  - Interdependencies and Resource Requirements
- Applied activity: Learners are given a short description of three systems in a small organization, with brief impact statements, and rank them by criticality, then assign a reasonable recovery time objective to each.

Module 4: Step 3: Preventive Controls

- Lessons:
  - What a Preventive Control Is, and Why Prevention Comes Before Recovery
  - Common Preventive Controls: Backups, Redundancy, and Power
  - Matching Controls to Identified Risks
- Applied activity: Learners review a short list of risks identified for a described system and select the most appropriate preventive control for each one.

Module 5: Step 4: Contingency and Recovery Strategies

- Lessons:
  - Backup Strategies and Data Recovery Options
  - Alternate Site Strategies: Hot, Warm, and Cold
  - Recovery Strategies for Cyber Incidents, Including Ransomware
  - Choosing a Strategy That Fits the Budget and the Risk
- Applied activity: Learners are given a short scenario describing an organization's budget and risk tolerance and select the most appropriate combination of backup and alternate site strategy, explaining the tradeoff of the option they did not choose.

Module 6: Step 5: Developing the Information System Contingency Plan

- Lessons:
  - What Belongs in a Contingency Plan Document
  - Activation and Notification Procedures
  - Recovery Procedures: Writing Steps Someone Else Can Follow
  - Reconstitution: Returning to Normal Operations
- Applied activity: Learners review a short, vague recovery procedure step and rewrite it as a clear, specific instruction that a different team member could execute without additional context.

Module 7: Step 6: Testing, Training, and Exercises

- Lessons:
  - Why an Untested Plan Is Not a Plan
  - Types of Exercises: Tabletop, Walkthrough, and Functional
  - Training the People Who Will Execute the Plan
- Applied activity: Learners are given a short scenario describing an organization that has never tested its plan and recommend which type of exercise to start with and why.

Module 8: Step 7: Plan Maintenance and Building Lasting Cyber Resilience

- Lessons:
  - Keeping a Contingency Plan Current
  - What Triggers a Plan Update
  - From a Single Plan to an Organizational Resilience Program
- Applied activity: Learners review a short list of organizational changes, a new critical system, a staff turnover in a key role, a completed exercise with findings, and identify which ones should trigger a plan update and why.