



COURSE / WORKSHOP: ccTLD Training Workshop - Attack and Contingency Response Planning (ACRP)

COURSE OVERVIEW: (20 Hours) Survey of methods and best practices for assessing operational risks faced by country code top-level domain (ccTLD) organizations that leverages the broader body of knowledge on risk assessment and management, business continuity planning and impact assessment, and disaster response and recovery. The course includes in-class group exercises to focus on techniques and tools for preparing a basic attack and contingency response plan. Special interest topics include case studies, formulating a contingency communications plan for a ccTLD, and a primer on cyber threats and mitigation strategies addressing DDoS attacks.

TOPIC	HOURS	DESCRIPTION
Case Studies/Overview - Contingencies and the Philosophy of Preparation	2.5	Introduces technical and non-technical impacts of disasters and cyber attacks using real-world examples. Details the need for effective risk assessment and planning, and potential impact if these activities are not performed.
Risk Assessment - Identifying Business Objectives	1	Introduces the need to focus planning efforts on those critical business objectives that are most important to an enterprise. Identifies best practices for initiating a planning process and techniques for determining business objectives of an organization.
Risk Assessment - Determining Critical Assets and Operations	1	Presents a methodology and associated templates for guiding an enterprise through the task of identifying critical information assets, operations, and key activities as they relate to the overall critical business objectives.
Risk Assessment - Threats, Vulnerabilities, and Impact	3	Introduces the basic risk equation – $RISK=THREAT \times VULNERABILITY \times IMPACT$. Discusses threat and vulnerability in the context of critical information assets and operations, and defines impact as it applies to critical business objectives. Presents a methodology and associated templates for guiding an enterprise through the task of identifying threats to and vulnerabilities of critical information assets.
Risk Assessment - Analyzing Risk	0.5	Presents a methodology and associated templates for guiding an enterprise through the task of performing a qualitative risk analysis using identified critical information assets and key business objectives.
Contingency Planning - Mitigation Strategies and Activities	1	Provides an orientation to different mitigation strategies, including assuming, transferring, and limiting impact and vulnerabilities. Highlights industry practices for alternate sites and mutual aid agreements.
Contingency Planning - Documenting a Plan	1	Presents overview of the contents of a contingency plan and a template for use in documenting an enterprise contingency plan.
Contingency Planning - Evaluating and Exercising a Plan	0.5	Considerations and options for planning, conducting, and assessing contingency plans. Covers basic concepts of plan reviews, structured walk-through, table-top exercises, functional, and operational exercises.
Practical Exercise: Risk Assessment of ccTLD Operational Environments	7	Series of small group sessions which use the ACRP templates to perform a notional risk assessment of general ccTLD operations.
Special Topic: Cyber Threats to ccTLD Operations	1.5	Presents current and emerging cyber threats to ccTLD operations and infrastructure. Identifies possible mitigation options.
Special Topic: Response Communications Planning	0.5	Overview and discussion of best practices for communicating with the public and key stakeholders during a contingency.
Special Topic: Mitigation of DDOS Attacks Using Anycast	0.5	Companion to the cyber threat special topic. Presents overview of <i>anycast</i> and reasons for implementing the configuration to mitigate DDOS attacks.