The Institute for Homeland Security at Sam Houston State University is please to offer the following Certificate of Completion (for attending 8 select sessions) at the SORM Continuity Symposium, July 31 to August 2, 2024, SHSU The Woodlands Center, The Woodlands, Texas.

Attendees must attend each of the 8 sessions as described below.

For more information, contact: Robert Crane at IHS, rec057@shsu.edu

---

Title: "Critical Infrastructure Resiliency and Continuity"

Sessions' Title, Descriptions, and Learning Objectives.

Session 1. Preparing for Natural Hazards. Factoring in Climate Trends.

Daniel Reilly, Warning Coordination Meteorologist
National Weather Service, Houston, Texas

Description: This presentation from the National Weather Service will focus on a description of natural hazards that should be considered when developing COOP plans with some discussion on how the frequency and intensity of these various hazards may evolve with future climate change. This is a fairly young science. There is some uncertainty, but will present the scientific consensus on future trends in various types of natural disasters.

Learning Objectives:

1. Better understand natural hazards in Texas and how they can disrupt business operations.
2. Describe how different hazards and impacts are distributed across the state.
3. Learn the basic science behind climate change and how a changing climate may impact various natural hazards. This would include hurricanes, heat waves, floods, drought, etc.
4. Climate science, attribution is an active area of research. Will present consensus view on hazard frequency, intensity changes, but also address the uncertainties, different viewpoints for each.

Session 2. Project Management Techniques for Business Continuity

Dr. Pamela J. Zelbst, Distinguished Professor, PMP
Director: Center for Innovation, Technology & Entrepreneurship
Sam Houston State University

Description: The basic definition of a project is a temporary, unique or progressive event that has a time period in which it is to be accomplished and has specific goals and objectives. Within organizations, a project generally results in or from changes that are necessary addressing issues related to a product, operational function, improvement or strategic implementation. In this session we will discuss the project techniques needed for business continuity and resiliency of the organization.

Learning Objectives:

1. Developing a vision of project continuity and why it is important to organization.
2. Addressing the characteristics of change (measurability, rationalization and implementation).
    a. Examining the triggers for resistance to change such as:
        i. Disorientation
        ii. Disidentification
        iii. Disenchantment
        iv. Disengagement
3. Understanding the relationship of project continuity and resiliency, adaptability and security.
4. Discuss tools for project continuity and resiliency.

Session 3. Cyber Incident Management Planning: A Practical Approach for Continuity Practitioners

Julio Gonzalez, Supervisory Protective Security Advisor, and
Jeremy Hansen, Protective Security Advisor, for Southeast Texas
Cybersecurity and Infrastructure Security Agency, Region 6
U.S. Department of Homeland Security

Description: In this presentation, representatives from the Cybersecurity and Infrastructure Security Agency (CISA) will discuss the newly released *National Security Memorandum on Critical Infrastructure Security and Resilience*, and fundamental concepts, practices, and resources that contingency planners and continuity practitioners can utilize to develop a cyber incident response plans or annexes for their organizations.

Learning Objectives:

1. Understand CISA's organizational structure and security advisors' available resources.
2. Understand CISA's role as the National Critical Infrastructure Coordinator.
3. Define cyber/physical convergence and how to integrate cybersecurity teams into an Incident Command Structure.

Session 4. Texas Critical Infrastructure Threat Trends and Risk Management

Clint Ladd, Texas Critical Infrastructure Protection Coordinator, and

Marisa Brusuelas, Maritime Intelligence Analyst

Office of Critical Infrastructure Protection, Texas Office of Homeland Security
Texas Department of Public Safety

Description: This presentation from the Texas Department of Public Safety will examine critical infrastructure threats, recent incidents, vulnerabilities, and disruption consequences. The presenters will end by highlighting key state-level infrastructure protection activities and the resources available to external partners.

Learning Objectives:

1. Summarize threats and threat trends applicable to critical infrastructure assets in Texas
2. Examine critical infrastructure vulnerabilities and disruption consequences, particularly within the context of recent disaster incidents
3. Identify state-level critical infrastructure protection activities and resources that are relevant to public and private sector partners

Session 5. Emerging Technology and Continuity (Virtual)

Nick Reese, CEO, Triantha

Description: In a world where cyber incidents are a certainty, the continuity of operations across any sector is a premium. The rapid development and convergence of emerging technologies such as quantum computing, AI, and blockchain will have significant effects on your continuity planning. In this session, we will discuss the global context for emerging technology competition and what it means for your operations.

Learning Objectives:

1. Understand the global context for emerging technology competition and application.
2. Analyze specific technologies for their impact on continuity.
3. Synthesize technical information within the global emerging technology context.
4. Evaluate current continuity practices relative to emerging technology mission impact.

Session 6. The Evolving Resilience Mindset of Continuity Practitioners

Robert Crane, Program Executive for Public Sector and Energy Security
Institute for Homeland Security, Sam Houston State University

Description: Resilience is a skill that can be cultivated. Having a security and resilient mindset is now essential skill for the successful continuity practitioner/leader to help protect the reputation or image of their respective organization in the face of a looming crisis. A crisis can come from anywhere often emerging from an overlooked issue or series of problems and failures of management to act and address an external and internal matter. Possessing a resilience mindset seeks to contain the matter or developing situation at the earliest “time of opportunity” and prevent escalation into a crisis.

Learning Objectives:

1. Define common characteristics of mental modeling and resilience that can be cultivated and practiced.
2. Discuss types, turning points, and stages of a crisis.

3. Introduce an example of a “Mental Model of Resilience” as a strategy to adjust and overcome developing situations or crisis events.

Session 7. Lessons Learned in Creating and Maintaining BCP Engagement

Paul Morris, Director of Compliance and Insurance

Sam Houston State University

Description: Leading an organizational business continuity planning process and operationalizing the plan is an excellent first step. Moving forward, how do organizations maintain field-level engagement and ensure that business continuity plans are used and maintained? This presentation from the SHSU Office of Compliance and Insurance will explore strategies for maintaining engagement, review lessons learned from an organization-wide refresh of business continuity practices, and offers ways to shift organizations from “checking the box” to creating a lasting continuity culture.

Learning Objectives:

1. Summarize ways to assess the current business continuity culture of the organization.
2. Identifying which tools to use, considering the level of BCP maturity in the organization.
3. Discuss strategies for maintaining organizational engagement after launching the BCP.
4. Explore strategies for handling transition of BCP owners.

Session 8. Resilience Strategies for Assessing Critical Infrastructure Dependencies

Heberto Villarreal and Clyde Loll, Project Managers
Institute for Homeland Security, Sam Houston State University

Description: This session delves into the various elements that make up a critical infrastructure in security and resilience programs and explains how they can be integrated into an organization’s protocols. By using scenario-based "risk monitoring," potential risks can be detected early on and proper countermeasures can be taken. Ultimately, a strong and effective leadership and organizational system is vital to avoid severe business consequences.

Learning Objectives:

1. Provide tools for:
    a. Assessing critical infrastructure risks, threats, and vulnerabilities to prepare for any possible crises.
    b. Establishing effective crisis communications plans in resilience plans.
    c. Analyzing supply chain risks, interdependencies, and key failure points can serve as important decision-making tools.
    d. Distinguishing between disaster recovery, emergency management, risk management, business impact, and business continuity in order to fully incorporate these concepts into the crisis management.
    e. Assessing the crisis readiness of critical suppliers as an essential proactive management tool.