Advanced Skill Certificate in Loss Prevention and Asset Protection

Emergency Response and Crisis Management

Emergency Response and Crisis Management Glossary

A

Active Shooter: An individual who is engaged in killing or attempting to kill people in a confined and populated area, typically with a firearm.

Asset Protection: Measures taken to protect assets from harm or loss, including physical, informational, and financial assets.

Acronyms: Abbreviations formed from the initial components of a phrase or a word, such as FEMA (Federal Emergency Management Agency) or CPR (Cardiopulmonary Resuscitation).

B

Business Continuity: The planning and preparation undertaken to ensure that an organization can continue to operate in case of a disaster or crisis.

C

Command Center: A centralized location where emergency response and crisis management activities are coordinated and managed.

Communication Plan: A detailed strategy outlining how information will be disseminated during an emergency or crisis to ensure clear and effective communication.

Crisis Management: The process of preparing for, responding to, and recovering from a crisis or emergency situation in a structured and coordinated manner.

D

Disaster Recovery: The process of restoring an organization's operations and infrastructure to normal after a disaster or crisis has occurred.

Emergency Response: The immediate actions taken to address and manage an emergency situation to protect life, property, and the environment.

E

Evacuation Plan: A plan that outlines procedures for safely and efficiently evacuating a building or area in the event of an emergency.

Emergency Operations Center (EOC): A designated facility where key personnel gather to coordinate and manage emergency response and crisis management activities.

F

First Responder: An individual who is among the first to arrive and provide assistance at the scene of an emergency or crisis.

Fire Safety Plan: A plan that outlines procedures for preventing, responding to, and evacuating in case of a fire emergency.

G

Incident Command System (ICS): A standardized management system used to coordinate and manage emergency response and crisis management activities.

H

Hazard Vulnerability Analysis (HVA): A systematic approach to identifying and prioritizing potential hazards and vulnerabilities that could impact an organization.

I

Incident Response: The actions taken immediately following an incident to assess the situation, contain the damage, and begin the recovery process.

J

Joint Information Center (JIC): A location where public information officials from multiple agencies or organizations coordinate and disseminate information during a crisis.

K

Known Threats: Potential risks or hazards that are identified and understood before they occur, allowing for pre-planned responses and mitigation strategies.

L

Loss Prevention: The practice of reducing the risk of loss or harm to people, property, or assets through proactive measures and strategies.

M

Mass Casualty Incident (MCI): An incident in which a large number of casualties require medical attention, often overwhelming local resources.

N

National Incident Management System (NIMS): A comprehensive, national approach to incident management that provides a framework for coordinating and integrating emergency response efforts.

O

Occupational Safety and Health Administration (OSHA): A federal agency that sets and enforces standards to ensure safe and healthy working conditions.

P

Personal Protective Equipment (PPE): Equipment worn to minimize exposure to hazards that can cause injuries or illnesses, such as gloves, helmets, and goggles.

Q

Quick Response: The swift and efficient response to an emergency or crisis to minimize damage, prevent further harm, and facilitate recovery.

R

Risk Assessment: The process of identifying, analyzing, and evaluating potential risks or hazards to determine their impact and likelihood of occurrence.

S

Situation Report (SITREP): A brief summary of the current status and developments of an incident or emergency situation, often used to communicate information to key stakeholders.

Security Measures: Precautions and practices implemented to protect people, property, or assets from harm, theft, or damage.

T

Threat Assessment: The process of identifying, evaluating, and addressing potential threats to an organization's security, operations, or personnel.

U

Unified Command: A coordinated approach to incident management in which multiple agencies or organizations work together under a single command structure.

V

Vulnerability Analysis: The process of identifying weaknesses in an organization's security, operations, or infrastructure that could be exploited by threats or hazards.

W

Warning Systems: Systems and procedures put in place to alert individuals of potential threats or hazards, such as sirens, alarms, or notifications.

X

Xenophobia: A fear or hatred of strangers or foreigners, which can lead to discrimination, prejudice, or violence in emergency or crisis situations.

Y

Yellow Command: A condition indicating that a hazardous situation exists and that emergency response and crisis management measures are being implemented to address the threat.

Z

Zero Day Attack: A cyber attack that exploits a previously unknown vulnerability in a computer system or software, posing a significant threat to data security and operations.