Business Continuity: How to Keep City Departments in Business after a Disaster

Shannon Spence, PE

Red Oak Consulting, an ARCADIS group

ICMA

98th ANNUAL CONFERENCE

PHOENIX

Maricopa County

OCTOBER 7–10, 2012

Agenda

- Security, Resilience and All Hazards
- The Hazards Cycle and Some Definitions
- Continuity of Operations 101
- A role for Standards
- The IT component

Risk Framework Evolution

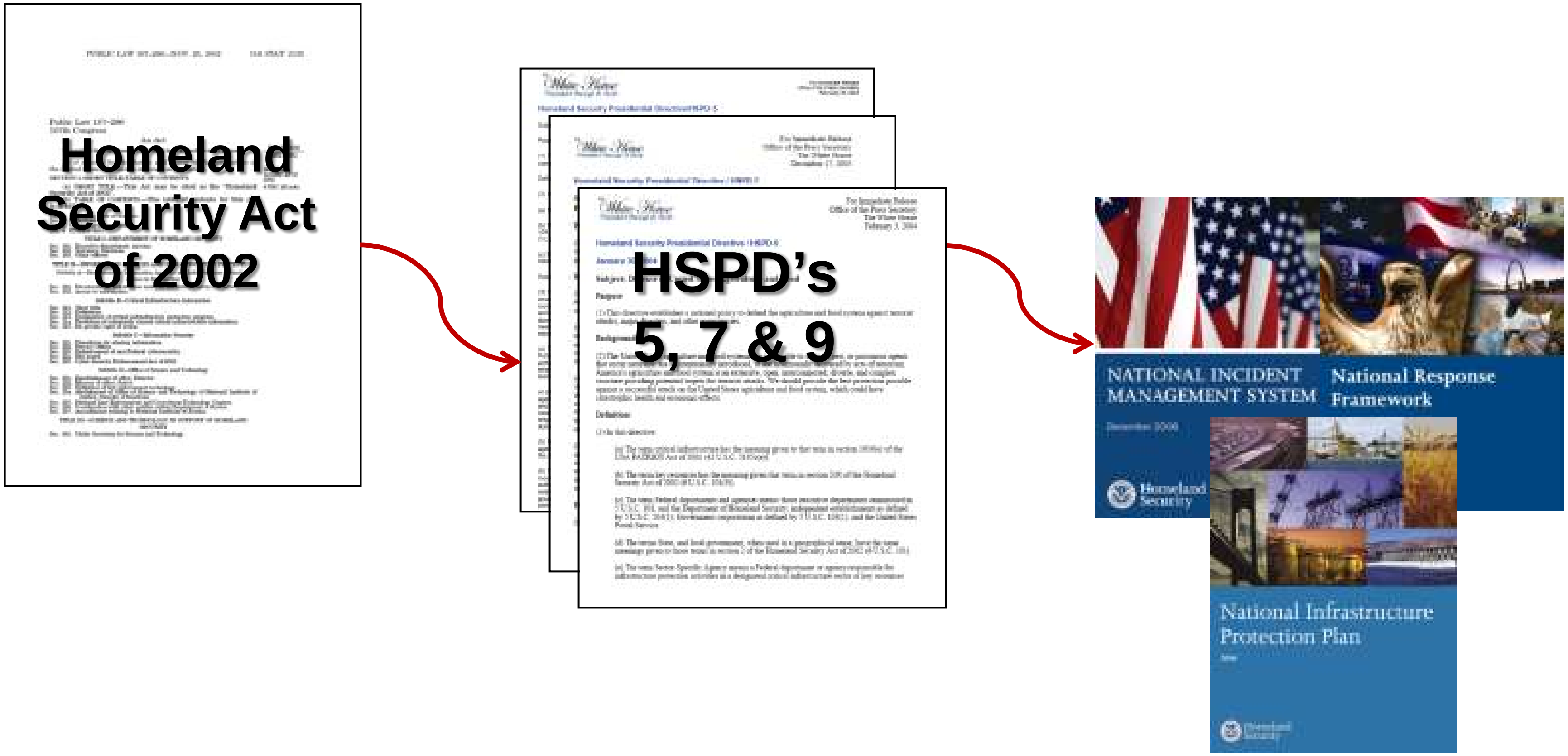
- Alfred P. Murrah Building, Oklahoma City (April 95)
  - Street closings around White House
  - New consideration of critical infrastructure vulnerabilities
- September 11, 2001
  - 2002 Bioterrorism Act = VA and ERP required for drinking water systems serving ≥ 3,300
  - Formation of Department of Homeland Security
  - Multiple Homeland Security Presidential Directives (HSPD’s)
- Hurricane Katrina (August 2005)
  - Paradigm shifts to All-Hazard
  - Confirms limits of guns-gates-guards model

Guns, Guards and Gates

Response, Recovery, Resilience

A McAllen strike force member begins the clean-up at a home in Galveston.

Key Drivers

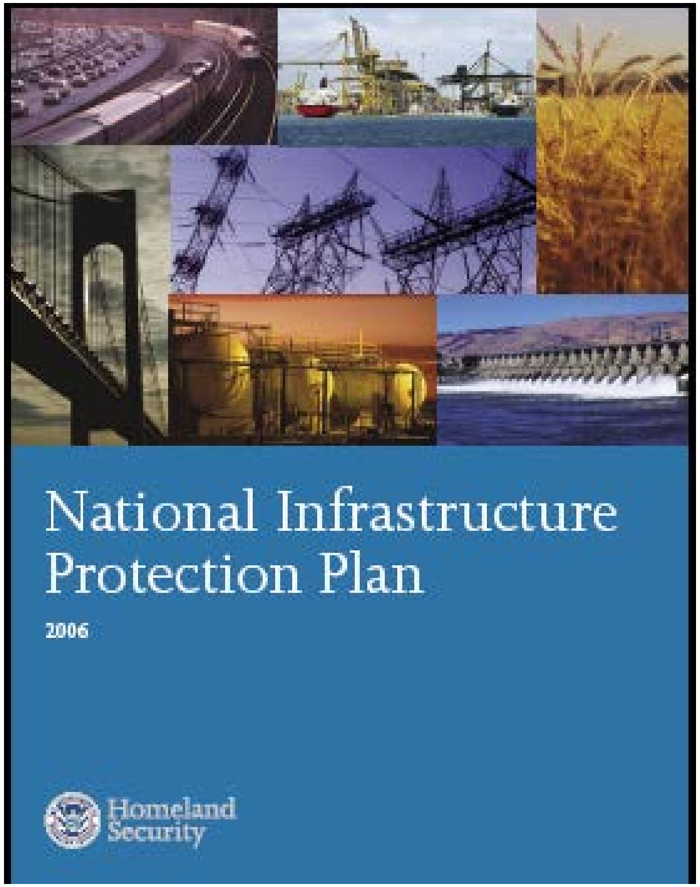


Homeland Security Act of 2002

HSPD's 5, 7 & 9

NATIONAL INCIDENT MANAGEMENT SYSTEM
December 2008
Homeland Security
National Response Framework
National Infrastructure Protection Plan
Homeland Security

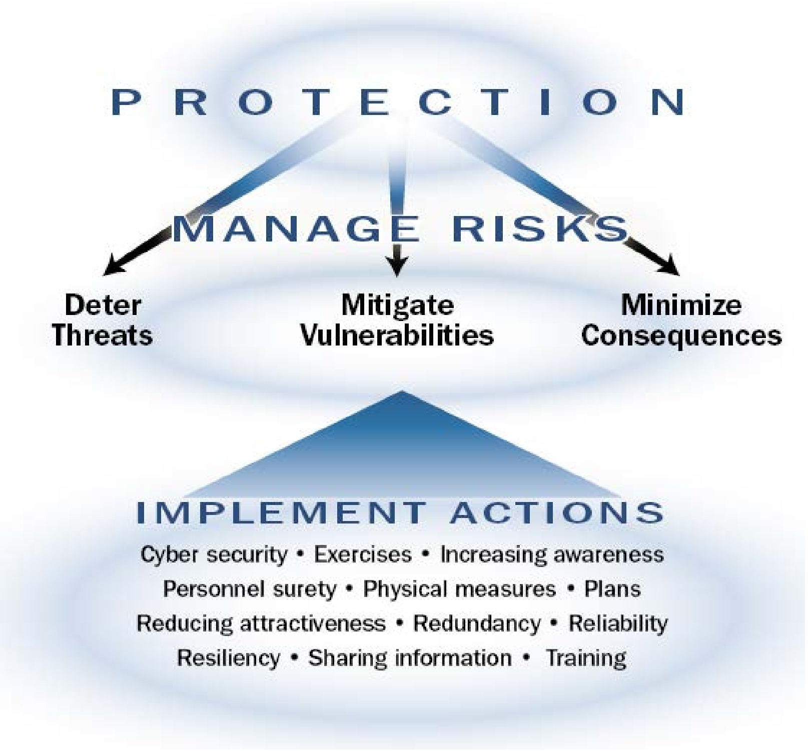
HSPD-7: The NIPP in Basic Terms



National Infrastructure Protection Plan

2006

Homeland Security



PROTECTION

MANAGE RISKS

Deter Threats

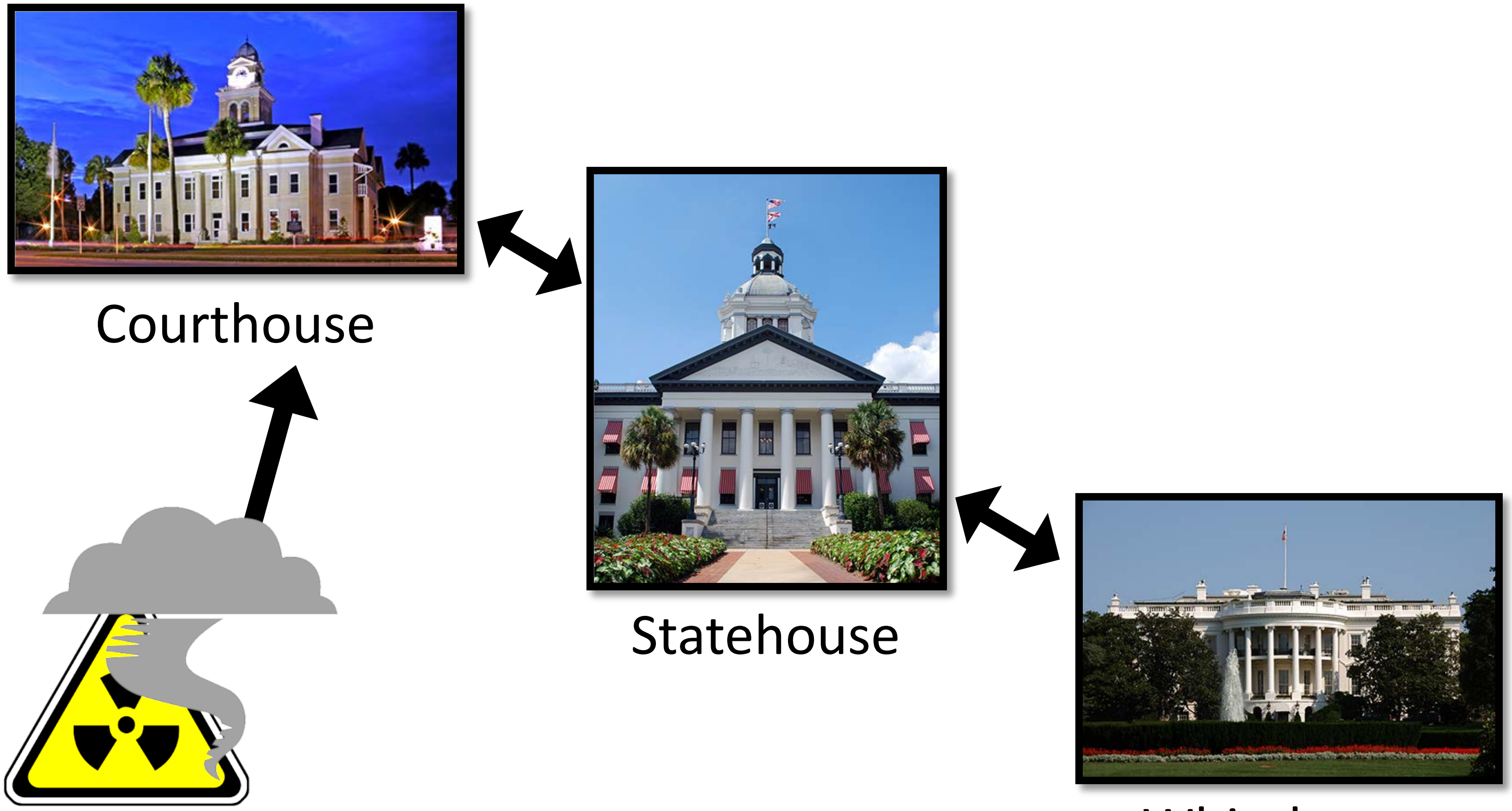
Mitigate Vulnerabilities

Minimize Consequences

IMPLEMENT ACTIONS

Cyber security • Exercises • Increasing awareness
Personnel surety • Physical measures • Plans
Reducing attractiveness • Redundancy • Reliability
Resiliency • Sharing information • Training

Incidents are LOCAL



Incident

Courthouse

Statehouse

Whitehouse

Potential Threats

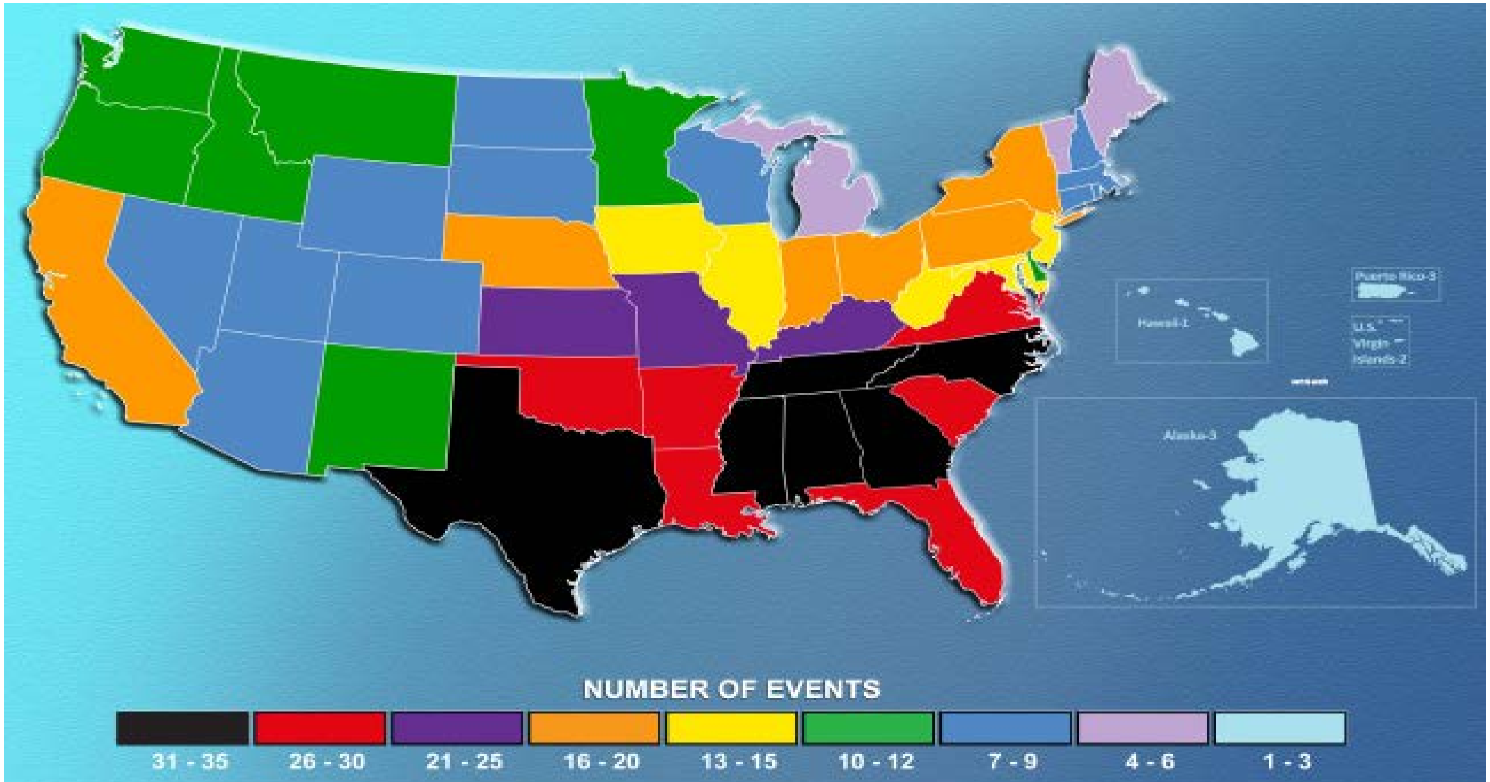
Natural	Man-Made	Both
Ice Storm Severe Winds Tornado Hurricane Earthquake Flood	Internet Virus Cyber Attack Agro-terrorism Chemical Explosion Water Poisoning Radiological Bio-Terrorism	Fire Disease

Incidents happen

And communities are impacted

And communities are impacted

Billion $ Events: 1980 - 2010



DISASTER TYPE	NUMBER OF EVENTS	PERCENT FREQUENCY	NORMALIZED DAMAGES (Billions of Dollars)	PERCENT DAMAGE
Tropical Storms/Hurricanes	27	27.2%	367.3	50.6%
Severe Weather	21	21.2%	41.4	5.7%
Heatwaves/Droughts	15	15.2%	185.2	25.6%
Non-Tropical Floods	15	15.2%	74.3	10.2%
Fires	10	10.1%	19.2	2.6%
Freezes	6	6.1%	18.6	2.6%
Blizzards	2	2.0%	11.9	1.6%
Ice Storms	2	2.0%	5.9	~0.8%
Noreaster	1	1.0%	2.2	~0.3%
	99		726.0	

*IMPORTANT NOTE: An event is counted if total damage estimate exceeds $1 billion dollars. A single event may affect multiple states.

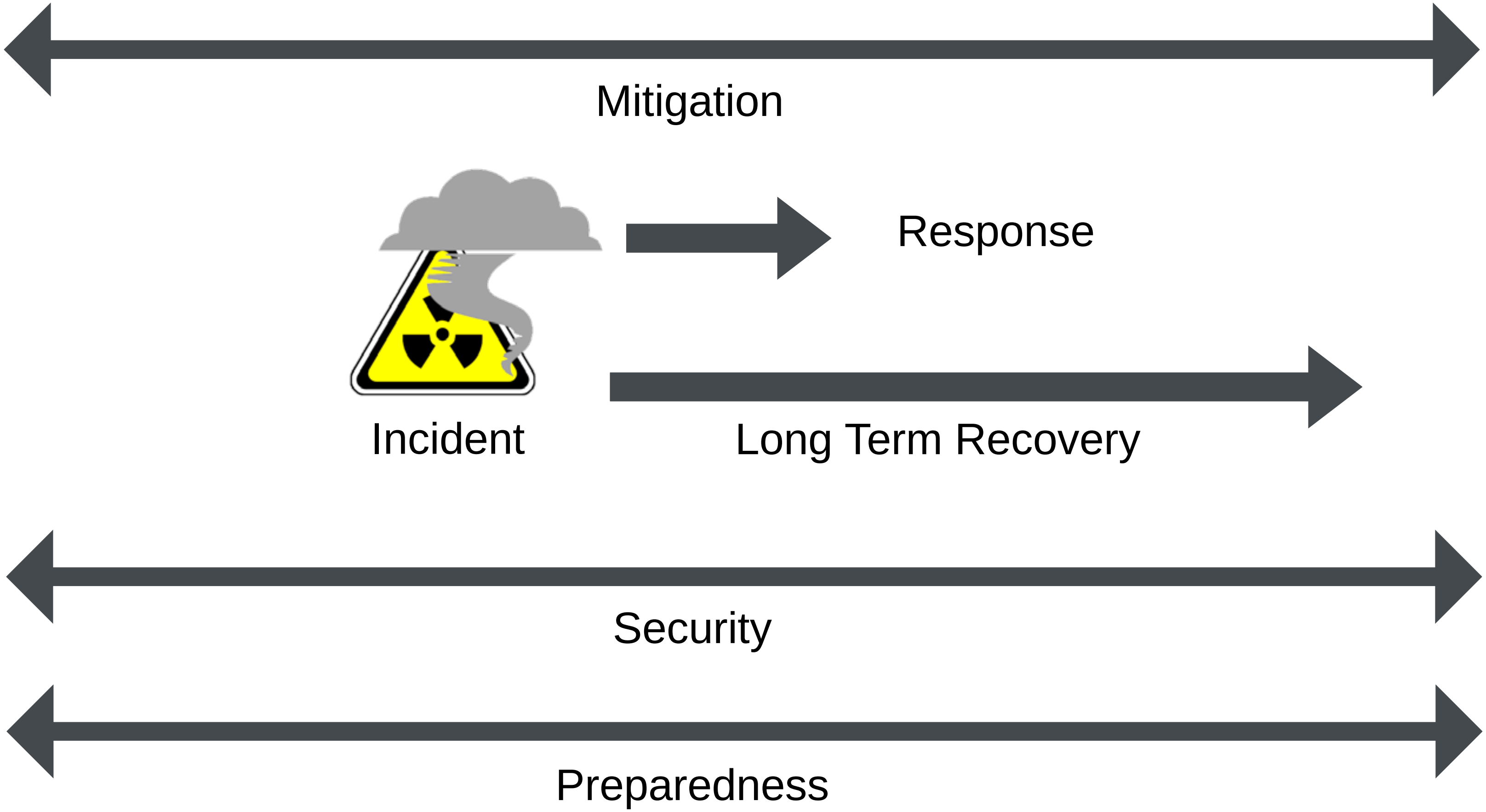
Source: NOAA's Climatic Data Center

Hopefully this is not the answer

Agenda

- Security, Resilience and All Hazards
- The Hazards Cycle and Some Definitions
- Continuity of Operations 101
- A role for Standards
- The IT component

Hazards Cycle



Mitigation

Response

Incident

Long Term Recovery

Security

Preparedness

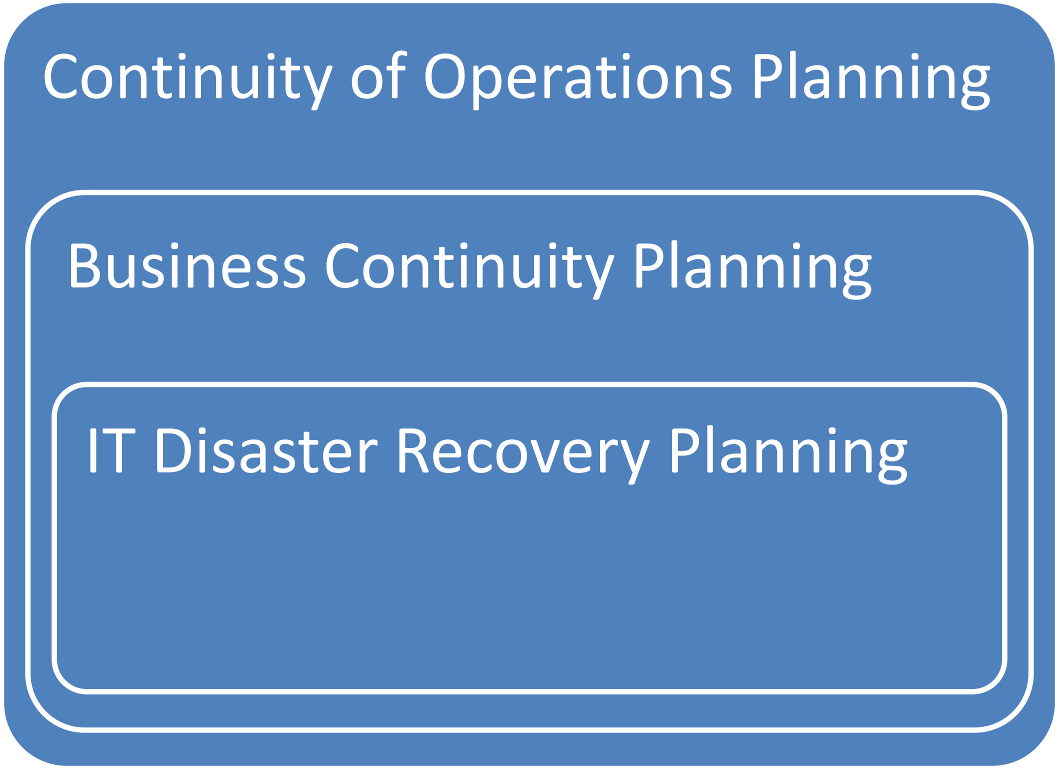
Definitions

- **Business Continuity Planning (BCP):** The effort to provide procedures to resume or restore **critical business processes** following a disruption.
- **Continuity of Operations Planning (COOP):** The effort to assure that **essential agency functions** across a wide range of potential emergencies continue.
- **Continuity of Government (COG):** **Preservation of the institution of government.** Maintaining leadership, delegation of authority and active command and control.

Agenda

- Security, Resilience and All Hazards
- The Hazards Cycle and Some Definitions
- Continuity of Operations 101
- A role for Standards
- The IT component

Layers of Planning



Continuity of Operations Planning

Business Continuity Planning

IT Disaster Recovery Planning

COOP Planning Objectives:

- Ensure the continuous performance of an agency’s **essential functions** during an emergency.
- Ensure the **safety** of employees.
- Protect **essential equipment**, records and other assets.
- **Reduce disruptions** to operations.
- **Minimize damage** and losses.
- Achieve an **orderly recovery** from emergency operations.
- **Identify relocation sites** and ensure operational and managerial requirements are met before an emergency occurs.

Critical Elements of a viable COOP Plan

- Essential Functions
- Delegations of Authority
- Orders of Succession
- Alternate Facilities
- Interoperable Communications
- Vital Records
- Human Capital Management
- Tests, Training and Exercises
- Devolution and Reconstitution

Essential Functions

- Those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the general public and sustain the industrial and economic base.

Delegations of Authority

- Who is authorized to make decisions or act on behalf of the department

Orders of Succession

- Provisions for the assumption of senior agency leadership positions during an emergency when the incumbents are unable or unavailable to execute their duties.

Alternate Facilities

- A location, other than the normal facility, used to conduct critical functions in the event that access to the primary facility is denied or the primary facility is damaged.

Interoperable Communications

- Provide the capability to perform essential functions, in conjunction with other agencies and organizations, until normal operations can resume.

Vital Records

- Records that if damaged or destroyed would disrupt organization operations and information flow, cause considerable inconvenience and require replacement or re-creation at a substantial expense.

Human Capital Management

- The process of acquiring, optimizing and retaining the best talent by implementing processes and systems matched to the organization’s underlying mission.
- Critical in ensuring the flexibility required of key personnel during these times of crisis.

Tests, Training and Exercises

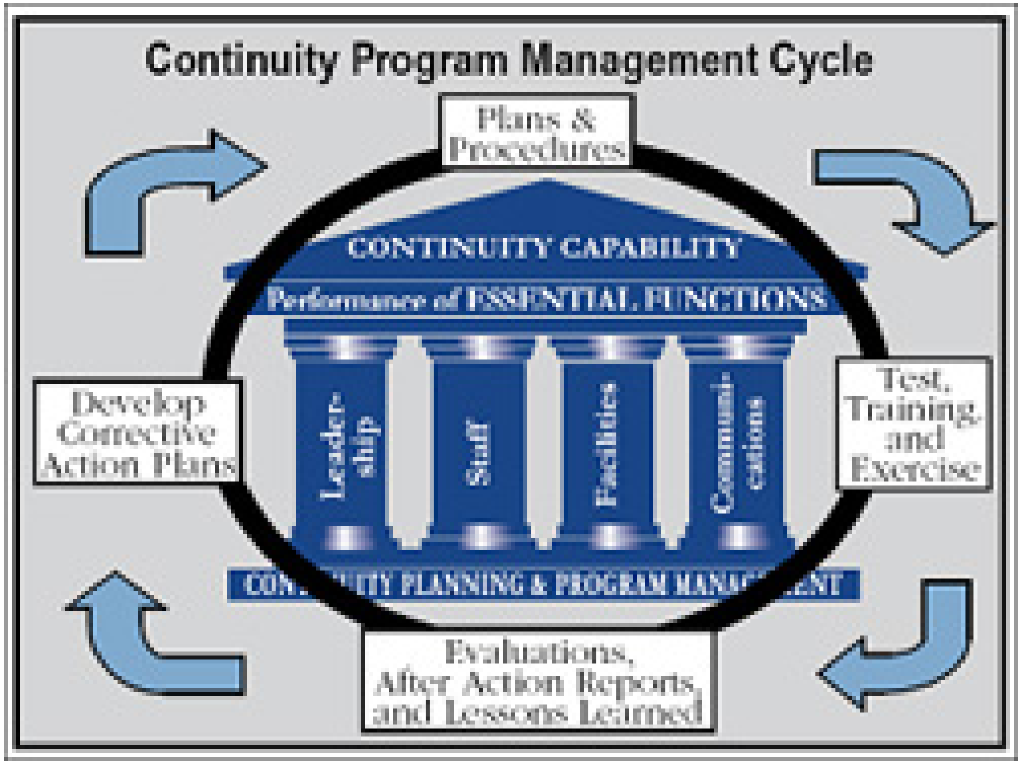
- All staff must be educated on their role in COOP plan execution.
- Exercises that simulate various disruptions and practice COOP plan execution must be conducted.

Devolution and Reconstitution

- The capability to transfer statutory authority for essential functions to other employees and facilities.
- The process to resume normal agency operations from the original or a replacement primary facility.

Phases of COOP Development

- Project Initiation
- Identification of Functional Requirements
- Design and Development
- Implementation
- Training, Testing and Exercises
- Revision and Updating


Continuity Program Management Cycle
Plans & Procedures
CONTINUITY CAPABILITY
Performance of ESSENTIAL FUNCTIONS
Leader-ship
Staff
Facilities
Communi-cations
Develop Corrective Action Plans
Test, Training and Exercise
CONTINUITY PLANNING & PROGRAM MANAGEMENT
Evaluations, After Action Reports and Lessons Learned

Agenda

- Security, Resilience and All Hazards
- The Hazards Cycle and Some Definitions
- Continuity of Operations 101
- A role for Standards
- The IT component

Standards: The Water Sector example

- G430-09: Security Practices for Operation and Management
- J100-10 Standard for Risk and Resilience Management of Water & Wastewater Systems
- G440*:* Emergency Preparedness Practices

G430-09:
Security Practices for Operations and Management

Purpose: This standard defines the minimum requirements for a protective security program for a water or wastewater utility that will promote the protection of employee safety, public health, public safety, and public confidence.

G430-09 :
Security Practices for Operations and Management

Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
l) Internal and External Communications
m) Partnerships
n) Verification

ANSI/AWWA G430-09:
Security Practices for Operations and Management

Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
l) Internal and External Communications
m) Partnerships
n) Verification

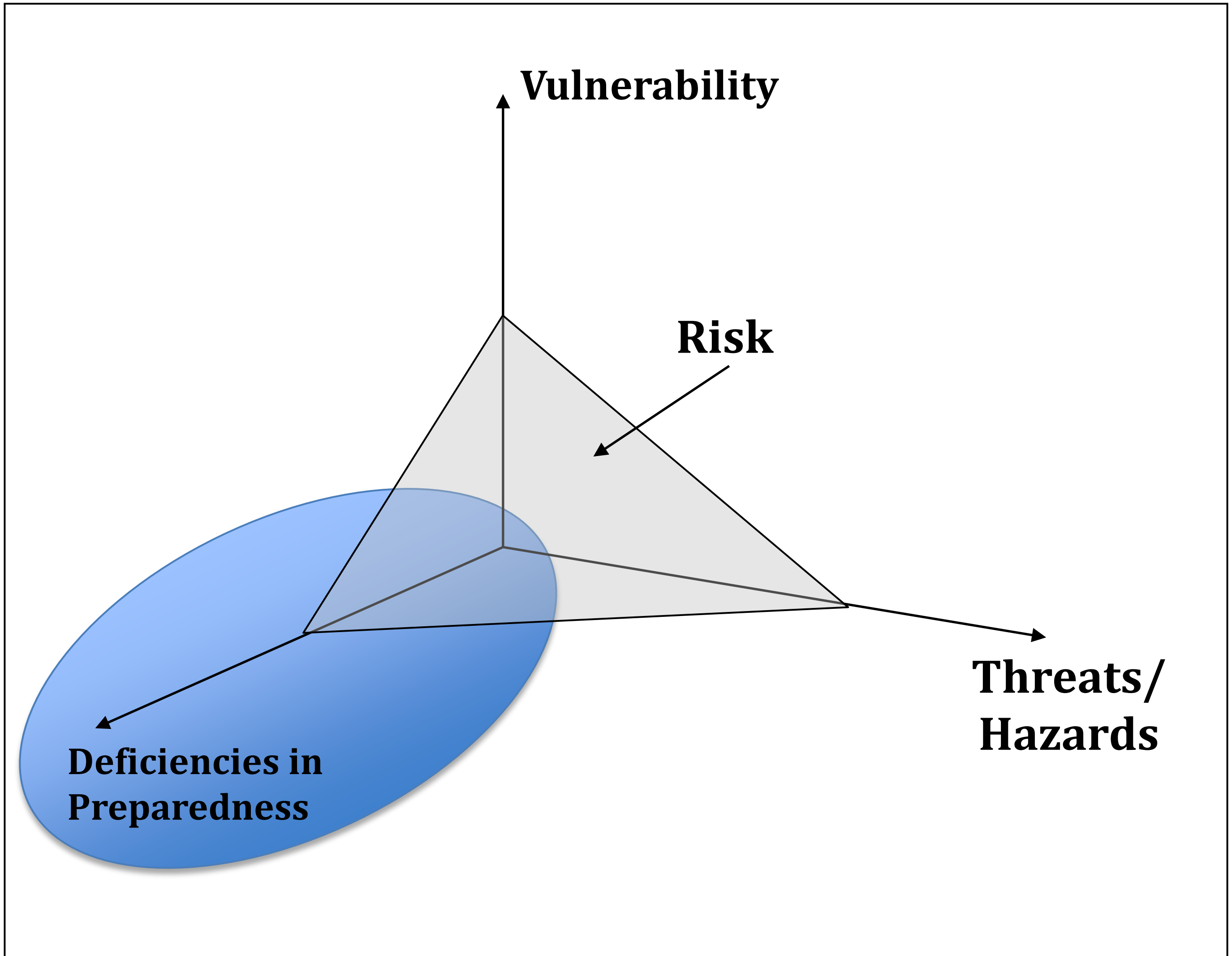
Standards: The Water Sector example

- G430-09: Security Practices for Operation and Management
- J100-10 Standard for Risk and Resilience Management of Water & Wastewater Systems
- G440: Emergency Preparedness Practices

Resilience is defined as:

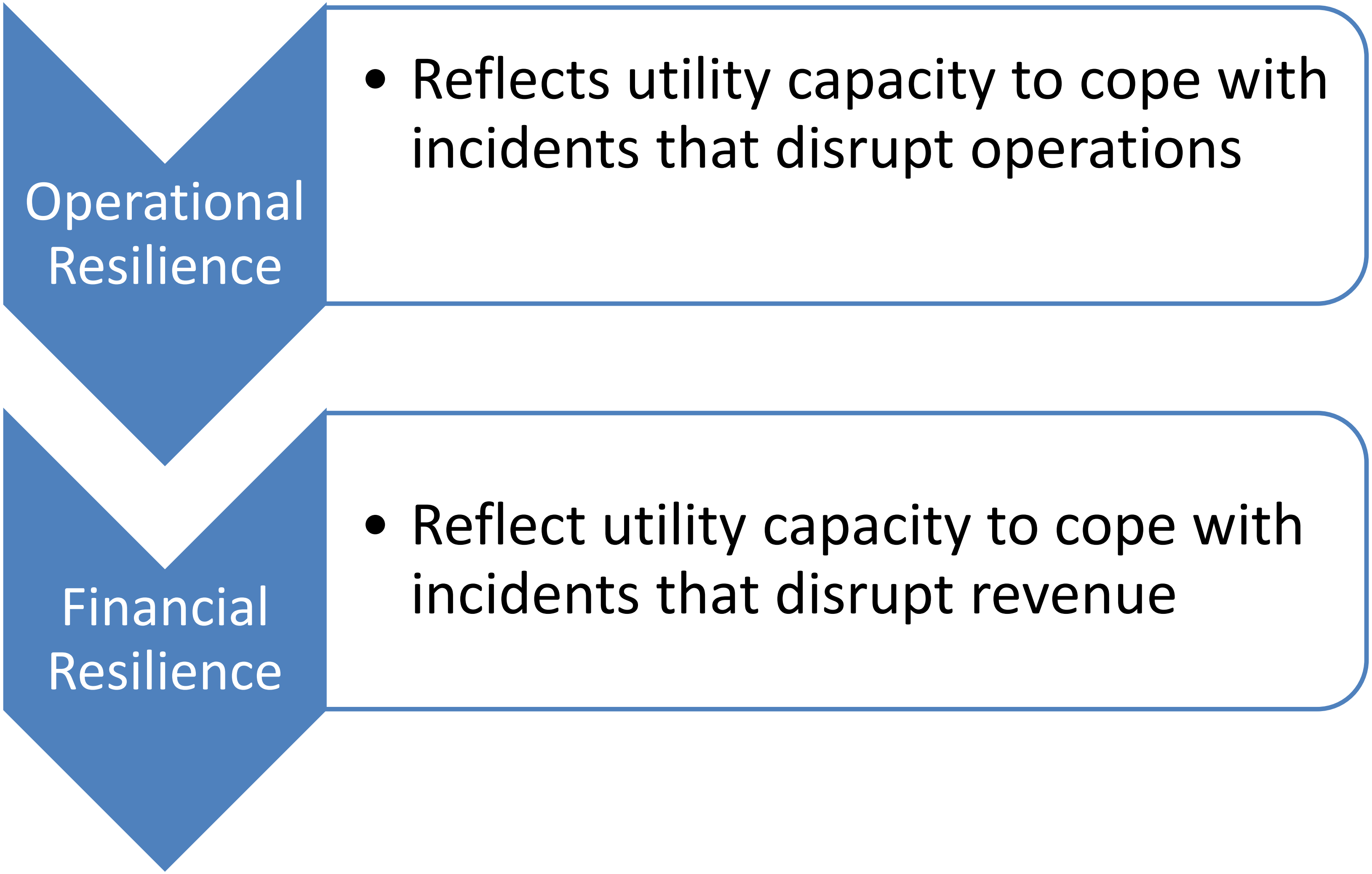
The ability to withstand and/or rapidly recover from an incident.

The Resilience Gap



Source: Villigran 2006

J100-10 Utility Resilience Index (URI)



Operational Resilience

- Reflects utility capacity to cope with incidents that disrupt operations

Financial Resilience

- Reflect utility capacity to cope with incidents that disrupt revenue

Sub-index Indicators

1. Emergency Response Plan
2. National Infrastructure Management Plan Compliance (NIMS, ICS)
3. Mutual aid and assistance agreements
4. Emergency power for critical operations
5. Critical parts and equipment
6. Critical staff resilience
7. Business Continuity Plan

Standards: The Water Sector example

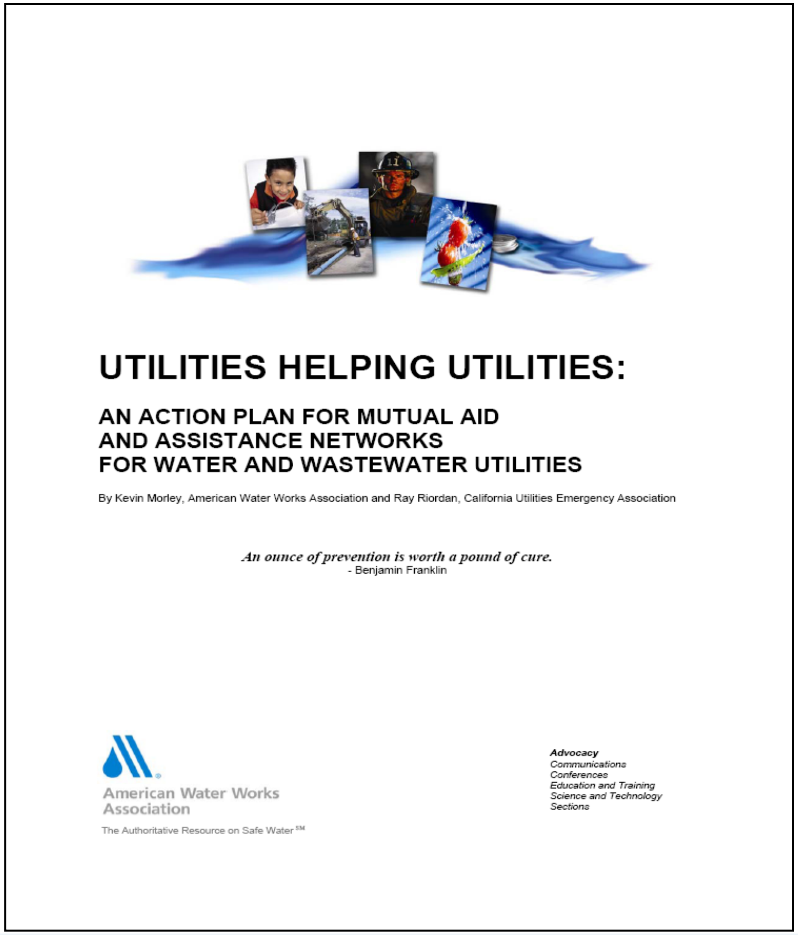
- G430-09: Security Practices for Operation and Management
- J100-10 Standard for Risk and Resilience Management of Water & Wastewater Systems
- G440*:* Emergency Preparedness Practices

G440-11: Emergency Preparedness Practices

Purpose: To define the minimum requirements for emergency preparedness for a water or wastewater utility, including the development of emergency response plan, exercising and updating.

Water/Wastewater Agency Response Network (WARN)

- **WARN Agreement**
  - **Voluntary**
  - **No Obligation**
  - **No cost**
  - **Liability/Workmans Comp**
  - **Reimbursement process**
  - **Element of NIMS**
  - **All-Hazards**



UTILITIES HELPING UTILITIES:

AN ACTION PLAN FOR MUTUAL AID
AND ASSISTANCE NETWORKS
FOR WATER AND WASTEWATER UTILITIES

By Kevin Morley, American Water Works Association and Ray Riordan, California Utilities Emergency Association

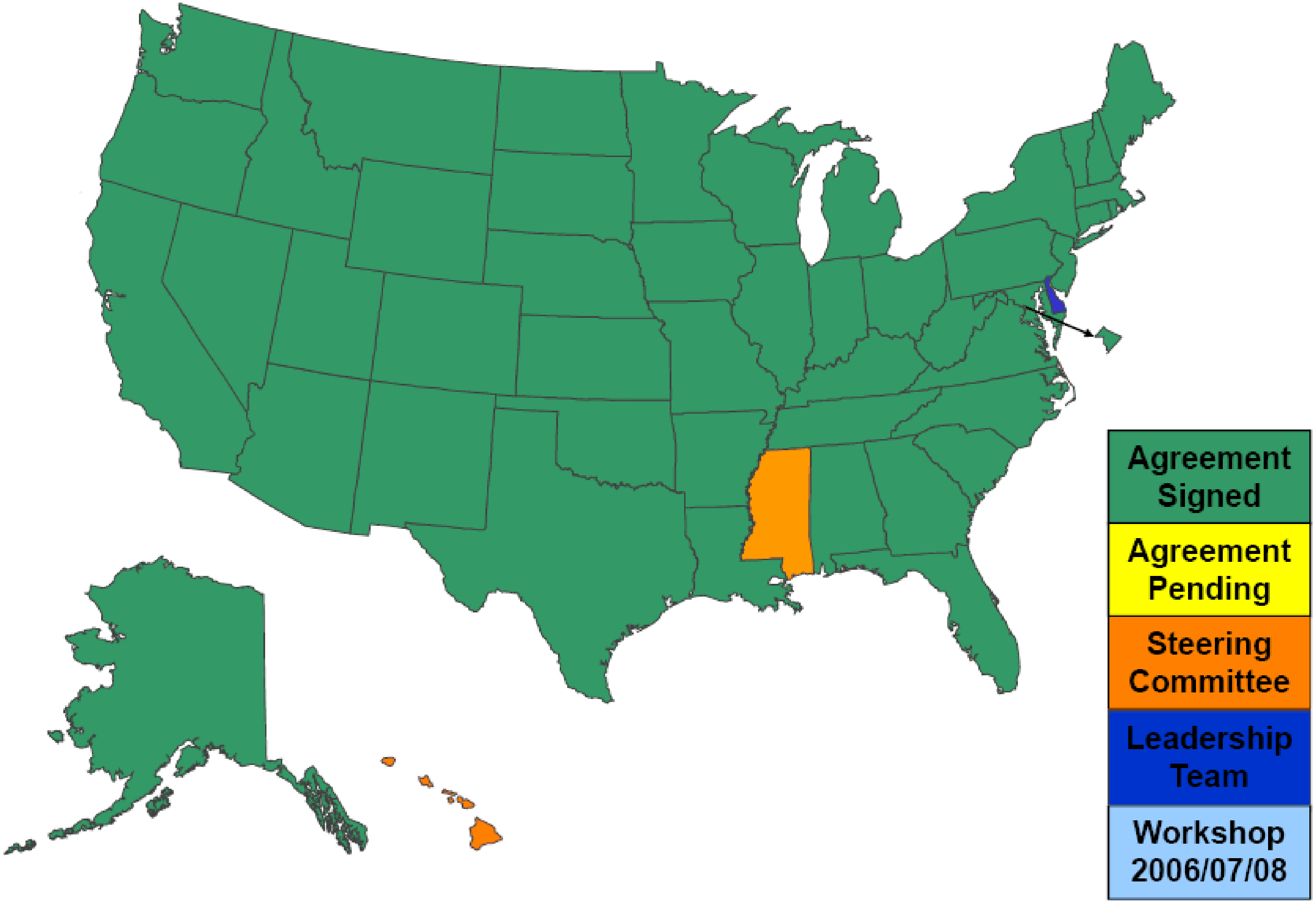
An ounce of prevention is worth a pound of cure.
- Benjamin Franklin

American Water Works Association

The Authoritative Resource on Safe Water SM

Advocacy
Communications
Conferences
Education and Training
Science and Technology
Sections

September 2011 (48)



Agenda

- Security, Resilience and All Hazards
- The Hazards Cycle and Some Definitions
- Continuity of Operations 101
- A role for Standards
- The IT component

Key Information Technology Trends

Business Environment

- Increasing need for real-time business information
- Further consolidation of small systems
- Aging workforce; staff turnover

Operations

- Increasing need for faster operational response
- Growing control and monitoring needs
- Increasingly stringent regulations
- Aging infrastructure

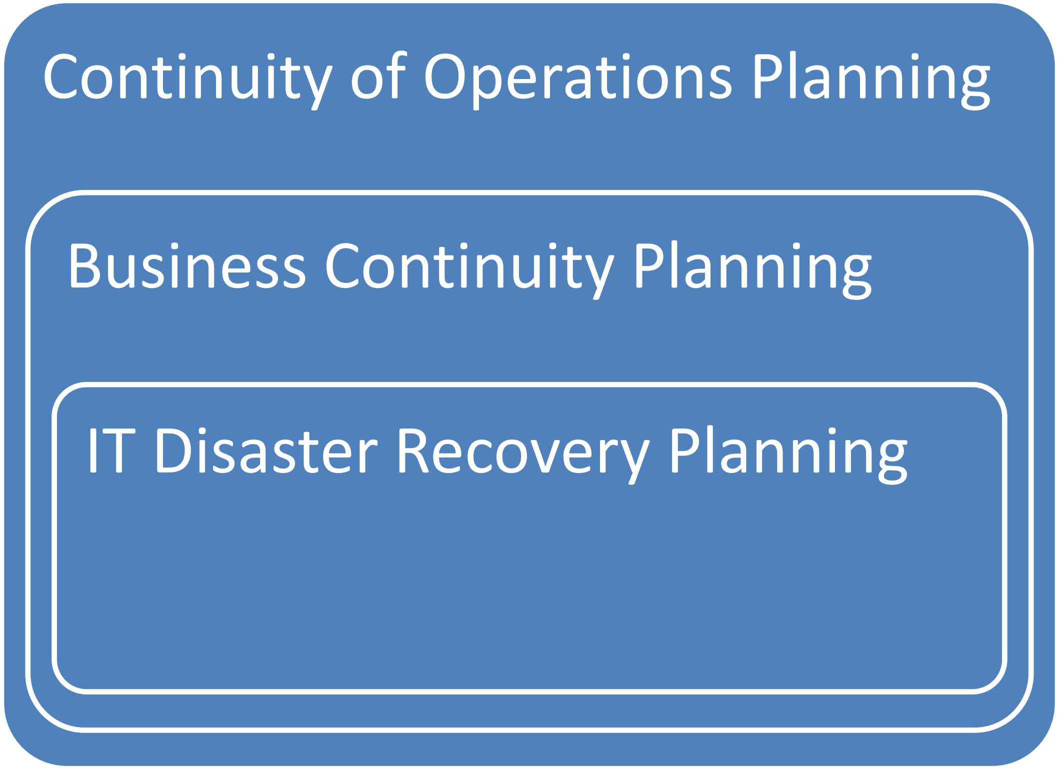
Societal

- Maintaining public confidence
- Changing infrastructure needs

Cyber Technology

- Convergence of information and operations technologies
- Increasing use of electronic & wireless communications
- More use of open non-proprietary systems
- Escalating cyber threats and accidents

Layers of Planning


Continuity of Operations Planning

Business Continuity Planning

IT Disaster Recovery Planning

Disaster Recovery Plan Goals

The disaster recovery process consists of defining rules, processes, and disciplines to ensure that the critical business processes will continue to function if there is a failure of one or more of the **information processing** or **telecommunications resources** upon which their operations depends.

http://www.sans.org/reading_room/whitepapers/recovery/disaster-recovery-plan_1164

IT DRP Planning Process

- Develop the planning group and set priorities
- Conduct the Business Impact Analysis (BIA)
- Conduct a Risk Assessment
- Develop Business Continuity and Recovery Strategies
- Develop Business Continuity Plan
- Implement plan
- Conduct awareness, testing, and training of the DRP
- Conduct Plan maintenance and exercises

Business Impact Analysis (BIA)

Defines objectives for the recovery of systems and application that support the business processes:

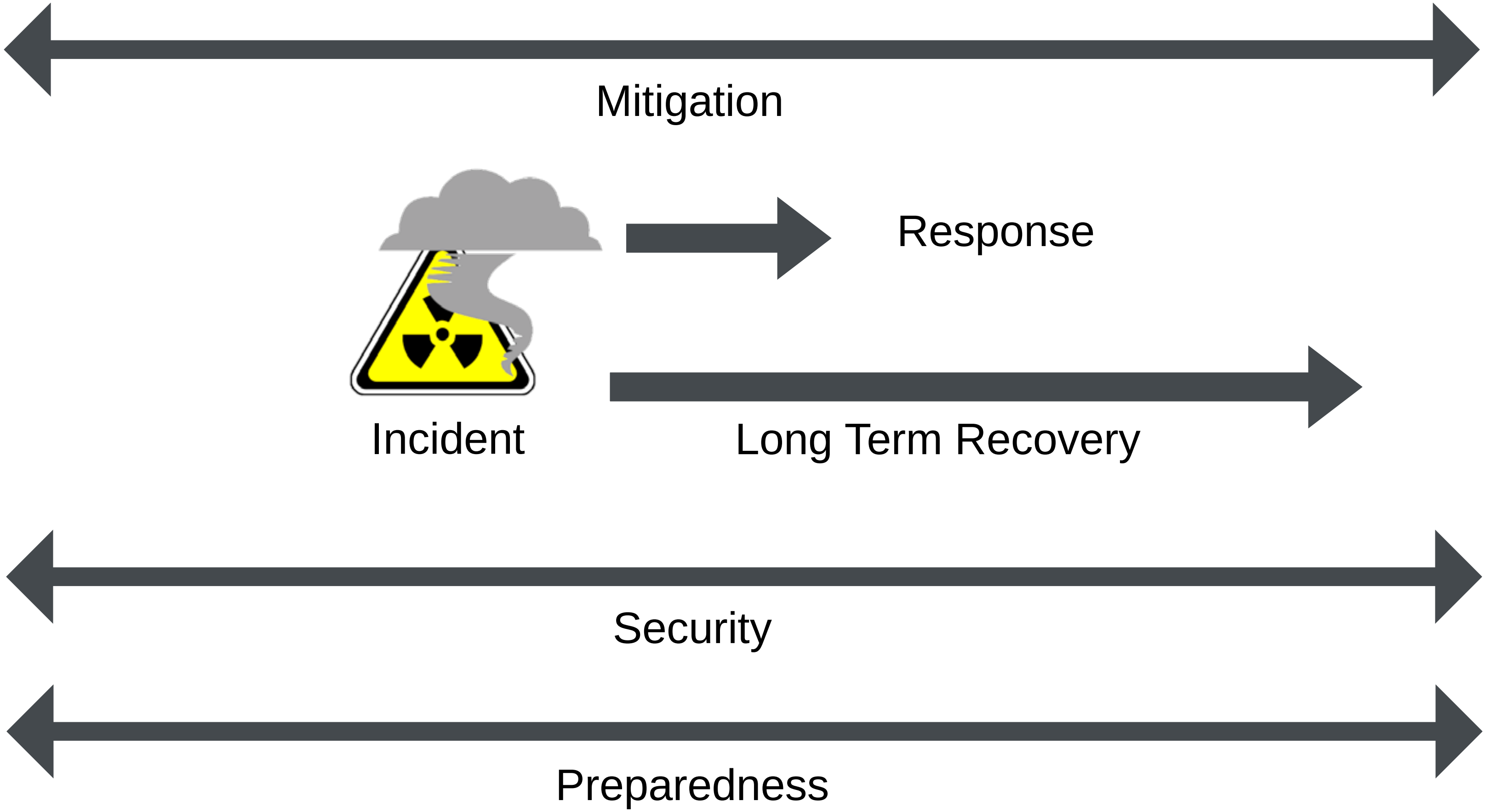
- Recovery Time: Number of hours/days to resume business process
- Recovery Point: Age of data to be restored

Map business processes to the system(s) that support them

Classification	Description
Mission Critical	✓Mission Critical to accomplishing the mission of the organization ✓Can be performed only by computers ✓No alternative manual processing capability exists ✓Must be restored within 36 hours
Critical	✓Critical in accomplishing the work of the organization ✓Primarily performed by computers ✓Can be performed manually for a limited time period ✓Must be restored starting at 36 hours and within 5 days
Essential	✓Essential in completing the work of the organization ✓Performed by computers ✓Can be performed manually for an extended time period ✓Can be restored as early as 5 days, however it can take longer
Non-Critical	✓Non-Critical to accomplishing the mission of the organization ✓Can be delayed until damaged site is restored and/or a new computer system is purchased ✓Can be performed manually

Incidents happen

Hazards Cycle



Mitigation

Response

Incident

Long Term Recovery

Security

Preparedness

Keep Going
Energizer

Questions/Comments?

Shannon Spence, PE

shannon.spence@arcadis-us.com

ICMA

98th ANNUAL CONFERENCE

PHOENIX

Maricopa County

OCTOBER 7-10, 2012

ICMA

98th ANNUAL CONFERENCE

PHOENIX

Maricopa County

OCTOBER 7–10, 2012