Continuity of Support Plan/ IT Contingency Plan

“It is a Dangerous World Out There, and information technology (IT) Leaders like Brain D. Voss (CIO Louisiana State University) know it.”

LINK: http://appl003.lsu.edu/itsweb/cioweb.nsf/$Content/ITS+in+the+Spotlight/$file/compworld07.pdf

Purpose

- Briefly review continuity of support planning/IT contingency planning definitions
- How they fit with business continuity planning and emergency preparedness
- Principles and Processes
- Federal Requirements

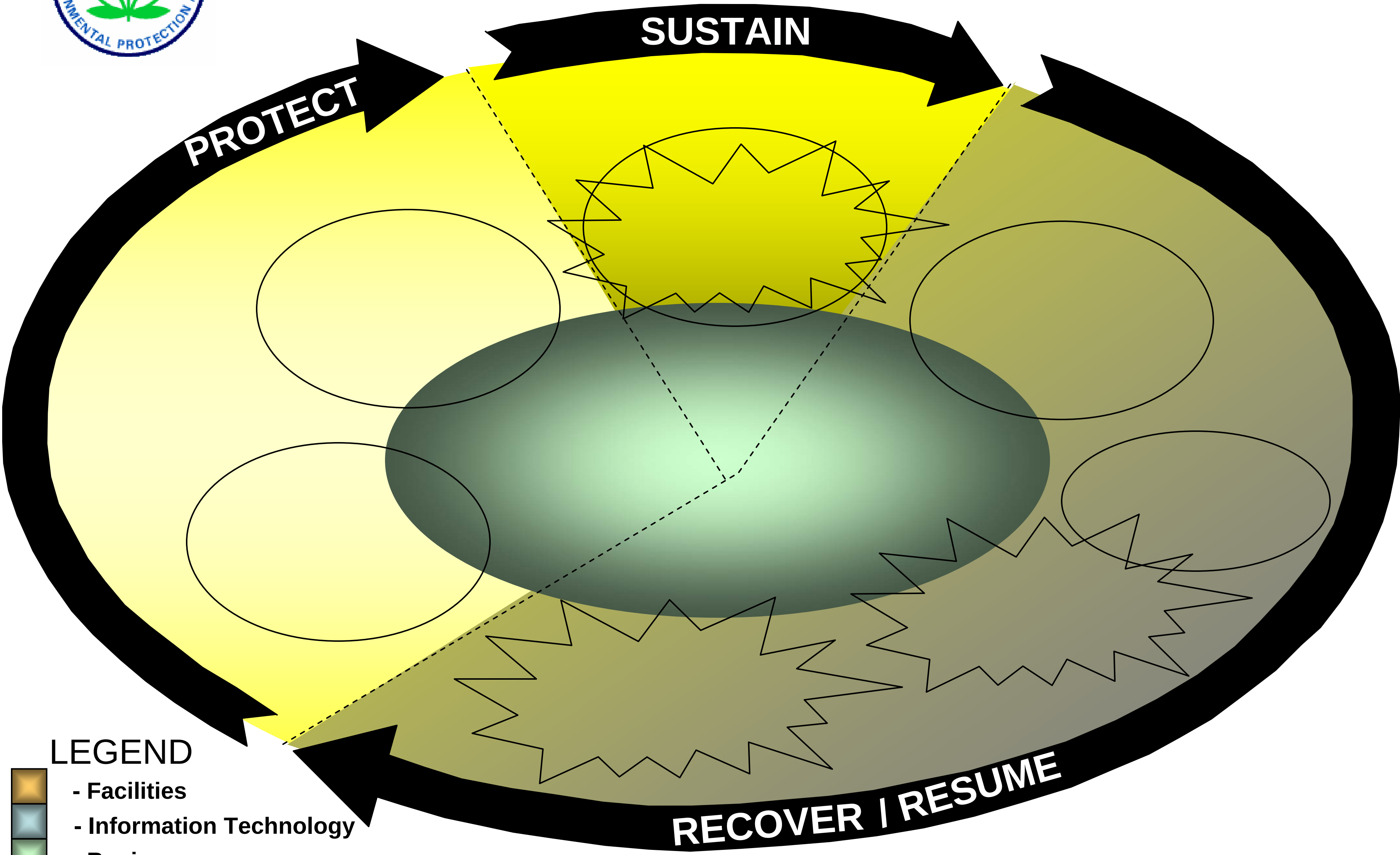
For Conference Purposes Only

Training Objectives

- Reviewing management responsibilities for Continuity of Support Planning/IT Contingency Planning
- Ensuring mission critical systems have adequate plans for recovery and resumption
- Analyzing business impacts if an IT system goes down
- Effectively testing adequacy of plans
- Where to go for more help

For Conference
Purposes Only

Emergency Preparedness



LEGEND

- 🟧 - Facilities
- 🟦 - Information Technology
- 🟩 - Business
- ✸ - Major Impact

Emergency Preparedness

- **Business Continuity Plan (BCP)**
  - Sustains business functions during and after disruption
  - Written for a specific or Key business process
  - IT systems considered in the BCP in terms of their support to the business processes
  - may not address long-term recovery of processes
  - may not return functions to normal operations (interim business continuity requirements)

- **Business Recovery Plan (BRP)**
  - Addresses the restoration of business process after an emergency.
  - procedures ensure continuity of critical processes throughout an emergency or disruption.
  - Coordinated with the DRP and can be appended to the BCP.

Emergency Preparedness

- **Continuity of Operations Plan (COOP)**
  - Restores essential functions at an alternate site
  - Performs those functions up to 30 days
  - Designed to support Headquarters elements
  - Developed and executed independently from the BCP (Mandated by PDD 67)

- **Continuity of Support Plan/ IT Contingency Plan**
  - Outline the procedures and capabilities for recovering from disruptions of service to a general support system or major application

Emergency Preparedness

- **Crisis Communication Plan**
  - Developed by the organization responsible for public outreach
  - Designates specific individuals as the only authority for answering questions from the public regarding disaster response
  - Includes procedures for disseminating status reports to personnel and to the public

- **Cyber Incident Response Plan**
  - Establishes procedures to address cyber attacks against an organization's IT system(s)
  - Designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents

Emergency Preparedness

- **Disaster Recovery Plan (DRP)**
  - Applies to major or catastrophic events that deny access to the normal facility for an extended period
  - IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site
  - Does not address minor disruptions that do not require relocation

- **Occupant Emergency Plan (OEP)**
  - Provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property
  - Developed at the facility level, specific to the geographic location and structural design of the building
  - The facility OEP may be appended to the BCP, but is executed separately

IT System Types

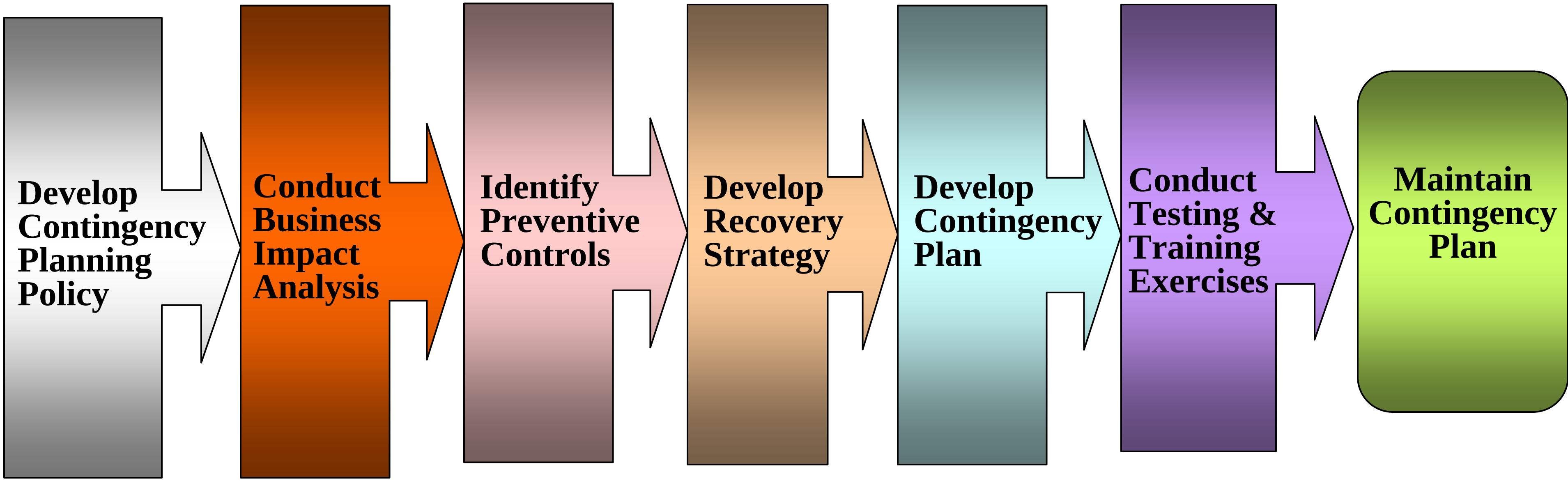
- **Systems Types**
  - **General Support Systems:** Interconnected set of information resources under the same direct management control that shares common functionality
  - **Major Applications:** Applications that require special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to (or modification of) the information in the application
  - **Minor Applications:** Other applications

For Conference
Purposes Only

Continuity of Support Plan
and
IT Contingency Plan
Defined

IT contingency planning refers to interim measures to recover IT services following an emergency or system disruption. It involves a coordinated strategy involving plans, procedures, and technical measures that enables the recovery of IT systems, operations, and data after a disruption

Contingency Plan Process



Develop Contingency Planning Policy

Conduct Business Impact Analysis

Identify Preventive Controls

Develop Recovery Strategy

Develop Contingency Plan

Conduct Testing & Training Exercises

Maintain Contingency Plan

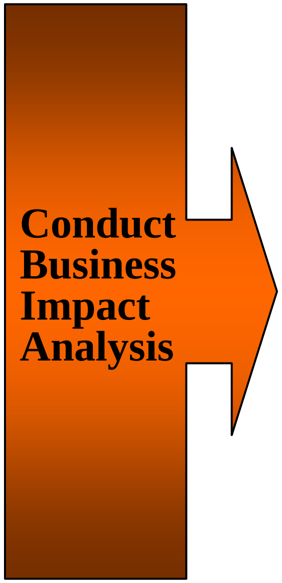
For Conference
Purposes Only

Step One - Planning Policy

Develop Contingency Planning Policy

- The Agency Network Security Policy requires IT system owners:
  - Develop, implement, and maintain a planning capability to address disruption of service to their IT systems
  - Document procedures for executing this capability
  - Incorporate documented procedures into their system security planning activities
  - Review and test their plans on an annual basis
  - Ensure all personnel are trained in the plan

Step Two – Conducting a Business Impact Analysis (BIA)



Conduct Business Impact Analysis

- Structured and disciplined process
- Identifies
  - Consequences & ramifications to the organization’s mission operations if an IT system goes down
  - Appropriate recovery steps and priorities when faced with system disruptions
- Characterizes system requirements, processes, and interdependencies
- Correlates specific system components with the critical services

Conducting a BIA

- Builds on Existing Security and Risk Management Activities
- System Categorization
- Threat & Vulnerability Identification

- For more information
  - The NIST SP 800-30 – ***Risk Management*** and NIST SP 800-60, ***Guide for Mapping Types of Information and Information Systems to Security Categories***

For Conference Purposes Only

System Categorization

Security Objective Adverse effect on individual or organizational operations or assets	Potential Impact: Low Limited	Potential Impact: Moderate Serious	Potential Impact: High Severe or Catastrophic
Confidentiality **Limit access** **Protect privacy**	Unauthorized disclosure → Limited harm	Unauthorized disclosure → Serious harm	Unauthorized disclosure → Severe harm
Integrity **Prevent change or destruction** **Ensure authenticity**	Unauthorized → change or ruin Limited → harm	Unauthorized → change or ruin Serious harm →	Unauthorized → change or ruin Severe harm →
Availability **Ensure timely, reliable access**	Disruption of access or use Limited harm	Disruption of access or use Serious harm	Disruption of access or use Severe harm

Threat & Vulnerability Identification

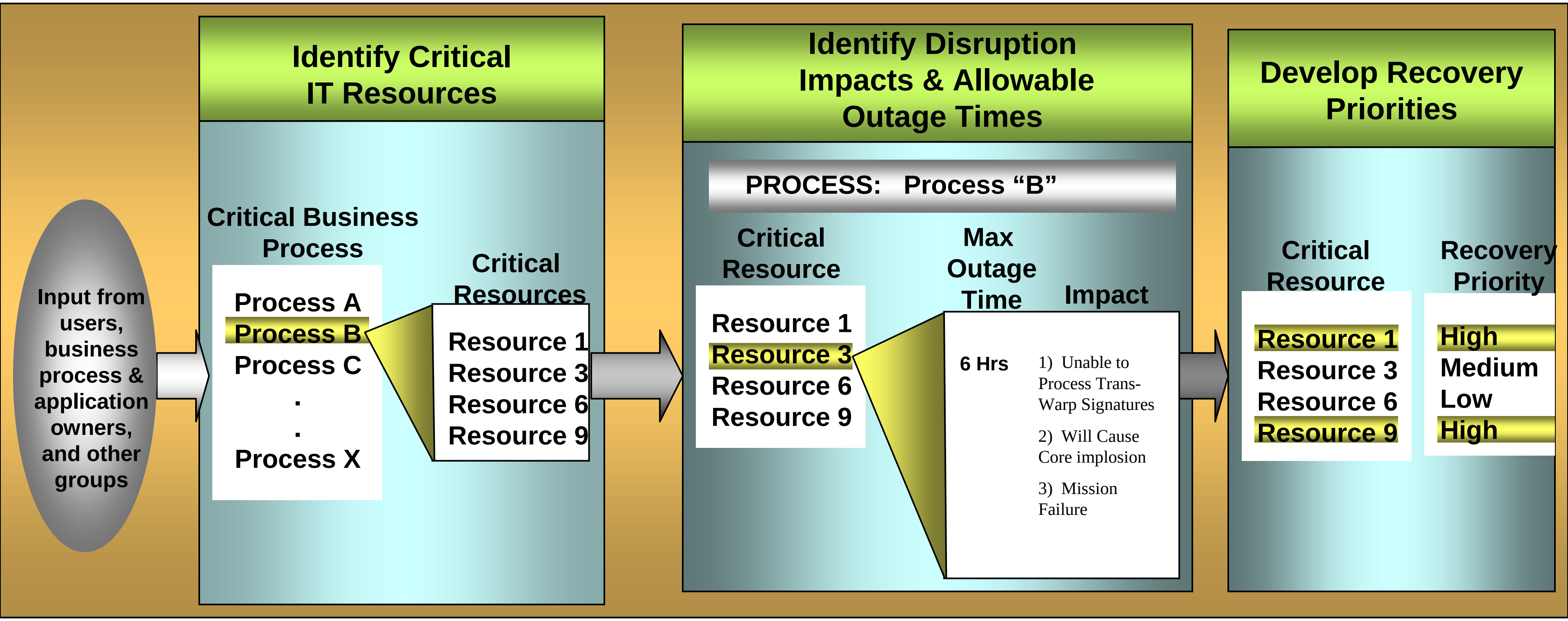
- Formal process that helps system owners and managers understand the extent to which their IT system is exposed to threats and vulnerabilities.
- Three classifications
  - – Natural - e.g., hurricane, torn
  - – Environmental - e.g., electric
  - – Human - e.g., operator error,

For Conference
Purposes Only

Threat & Vulnerability Identification

Threat or Vulnerability	Probability of Vulnerability Exploited	Potential Impact: Confidentiality	Potential Impact: Availability	Potential Impact: Integrity
Fire	Medium	Low	High	High
Hurricane	Low	Medium	Medium	Low
Hacker	High	High	High	High

Critical Resources Review



Input from users, business process & application owners, and other groups

Identify Critical IT Resources

Critical Business Process

Process A
Process B
Process C
.
.
Process X

Critical Resources

Resource 1
Resource 3
Resource 6
Resource 9

Identify Disruption Impacts & Allowable Outage Times

PROCESS: Process "B"

Critical Resource	Max Outage Time	Impact
Resource 1 Resource 3 Resource 6 Resource 9	6 Hrs	1) Unable to Process Trans-Warp Signatures 2) Will Cause Core implosion 3) Mission Failure

Develop Recovery Priorities

Critical Resource	Recovery Priority
Resource 1	High
Resource 3	Medium
Resource 6	Low
Resource 9	High

For Conference Purposes Only

Critical Resources Review Broken Down

- **Identify**
  - **IT resources such as hardware and software**
  - **System interfaces and/or connections**
  - **System information managers and operators**
  - **The business functions the IT system supports**
  - **Critical roles and responsibilities**

Critical Resources Review Broken Down

Resource Outage Matrix

- **Identify outage impacts and allowable outage times**
- **Characterize the impact on critical roles if a critical resource is unavailable; also**
- **Identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted**
- **Any cascading effects on the organization**

Critical Resources Review Broken Down

Resource	Outage Impact	Allowable Outage
Resource "A"	• Outage Impact 1 • Outage Impact 2 • Outage Impact "X"	Time in Minutes, Hours, Days
Resource "H"	• Outage Impact 1 • Outage Impact 2 • Outage Impact "X"	Time in Minutes, Hours, Days
Resource "X"	• Outage Impact 1 • Outage Impact 2 • Outage Impact "X"	Time in Minutes, Hours

Step Three –
Identify Preventive Controls

Identify Preventive Controls

- Uninterruptible power supplies
- Generators
- Air Conditioning
- Fire and smoke detectors as well as fire suppression equipment
- Water sensors
- Plastic tarps
- Heat resistant and water proof media containers
- Emergency master system shutdowns
- Encryption
- Frequent, scheduled back-ups
- Off site storage

Step Four - Develop Recovery Strategies

Develop Recovery Strategy

- Strategies to restore services including
  - – **Data Backup**
  - – **System Function Backup**
  - – **Alternate Sites**

Strategies should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents

Data Back Up

- System data should be backed up regularly
- Policies should specify the frequency of backups (e.g., daily or weekly, incremental or full), based on data criticality and the frequency that new information is introduced
- Policies should designate the location of stored data, file-naming conventions or encryption keys, media rotation frequency, and method for transporting data off

For Conference
Purposes Only

System Function Back Up

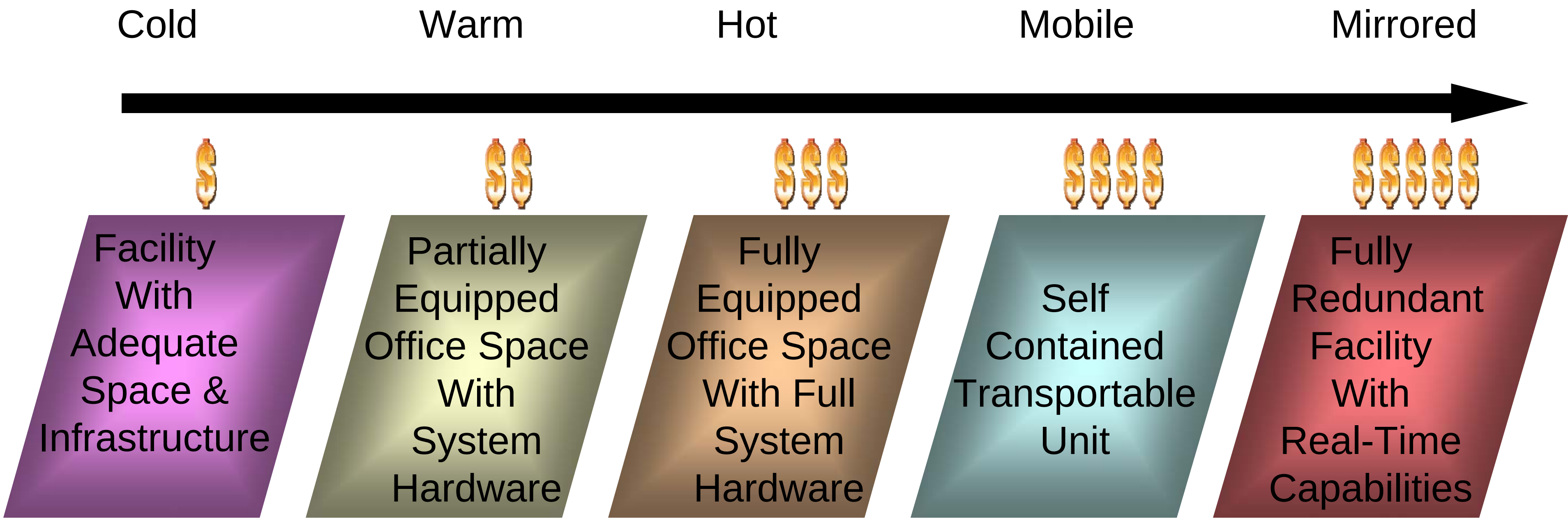
- The ability to reconstitute an IT system depends on being able to recover the data within an IT system’s unique functional environment
- Continuity of Support Plans/IT Contingency Plans must also seriously consider system functionality as an inseparable companion to data back up

Alternate Sites

- Geographic area - distance from normal operational location
- Accessibility - length of time needed to get to the site
- Security - ability to properly secure the data consistent with confidentiality requirements
- Environment - structural and environmental conditions
- Cost - cost of shipping and operational fees

For Conference
Purposes Only

SITE TYPES



Cold

$

Facility With Adequate Space & Infrastructure

Warm

$$

Partially Equipped Office Space With System Hardware

Hot

$$$

Fully Equipped Office Space With Full System Hardware

Mobile

$$$$

Self Contained Transportable Unit

Mirrored

$$$$$

Fully Redundant Facility With Real-Time Capabilities

Step Five - Document your Plans

Develop Contingency Plan

- Federal standards require
  - IT Continuity of Support Plans for GSS's
  - IT Contingency Plans for MA's
- Plans include
  - Detailed roles and responsibilities
  - Restoration procedures
  - Technical requirements for contingency operations

Plans Describe

- Concept of normal operations and emergency operations
- Roles and responsibilities
- Notification procedures
- Recovery procedures
- Plans describing how and when a system will return to normal operations (reconstitution phase)
- Assumptions which might affect the viability of the plan
- References or authorities requiring contingency planning
- Record of changes made to the plan due to the dynamic nature of today's IT environments

Step Six - Testing and Training

Conduct Testing & Training Exercises

- Periodic and regular testing, minimally ANNUALLY, to
  - Confirm effectiveness of the plan
  - Identify plan deficiencies
  - Evaluate the ability of the "recovery staff" to implement the plan quickly and effectively
  - Review for accuracy and completeness

Note: Ensure that test results are documented

Step Six - Training

- **Personnel identified in the plan must be knowledgeable and capable of carrying out the required task(s)**
- **Individuals need to either be trained in the procedures required to support the implementation of the plan, or, trained on the technology used in the solution**
- **Frequency of ”tooling the workforce” to support this mission requirement can coincide with the testing phase of the solution, i.e., on the job training**
- **Training requirements need to be captured, documented, and periodically assessed to stay current with technological refreshes**

Test Types

- Tabletop Exercises
  - Simulates an emergency situation in an informal, stress-free environment
  - Constructive discussion
  - Cost-effective method of testing crisis management plans, while causing minimal disruption to the organization.
  - Last from 2 to 4 hours or longer, depending on the issues discussed

For Conference
Purposes Only

Test Types

- Drills
  - – Drills are used to stimulate automatic responses to routine tasks during a crisis
  - – Drills are repetitive and are performed identically each time they occur
  - – Repetitive nature of drills prepares personnel to perform their duties automatically, even in situations of extreme duress

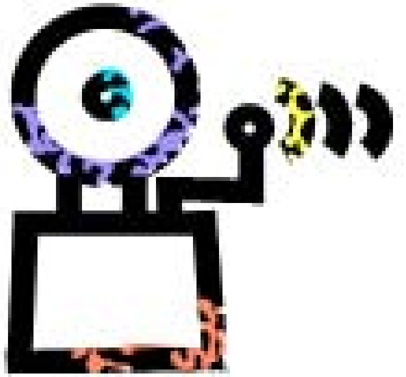
For Conference Purposes Only

Test Types

- **Functional Exercises:**
  - Fully simulated, interactive event
  - Focus on policies, procedures, roles, and responsibilities
  - Tests include one or more organizational functions in a time-pressured, realistic simulation
  - Scripts may be written for role player pretending to be external organizatio contacts
  - Possible relocation to the alternate si
  - Could last from 2 to 8 hours

Test Types

- **Full-Scale Exercises These**
  - **Focus on actual emergency conditions**
  - **Validate the capability to respond to an emergency**
  - **Focus on policies, procedures, roles and responsibilities that may be performed**
  - **Designed to verify the operational capabilities of an organization**



For Conference
Purposes Only

Step 7 – Maintain the Plan

Maintain Contingency Plan

✓Keep plan updated to reflect current

✓System status

✓Organizational structure

Federal standards recommend annual reviews for accuracy and completeness, occurrence of significant changes or for regular testing of the plan.

MANAGEMENT QUESTIONS

1. Ask for a briefing on your system's contingency plans.
2. Ask specific questions such as:

   a. How often is the data in the system backed up?
   b. Where is the back-up data stored?
   c. What kind of equipment do we need to get the system fully restored so that it is fully functioning?
   d. What software is installed at our back-up site?
   e. What telecommunications system do we need?
   f. If you own a Major Application, confirm who owns the underlying general support system?

3. Confirm/validate the Business Impact Analysis (BIA). Does the analysis correctly reflect your IT system's relationship with mission accomplishment?