



P U B L I C S E R V I C E S

IT Contingency Planning Workshop

brianfuller@kpmg.com, ext. 3581
bsizemore@kpmg.com, 962-0528

Planning for Survival (Icebreaker)

Scenario: As a group, you've been stranded in the desert, at least 100 miles away from any known civilization. The area is flat and barren, with the exception of a few barrel or saguaro cacti. Temperatures in the area are known to reach over 110 degrees. You're dressed in light-weight clothing, and have 15 items available to assist you.

We asked 100 former "Survivor" contestants the following question: What are the six most important items you would use to survive?

The moral of the story:

In order to best survive a calamity, it's best to

- **Plan for an event before it happens,**
- **Gather relevant subject matter expertise, and**
- **Understand the possible risks the situation may create, and address those risks.**

This workshop will enable you to:

- 1** *Understand the underlying contingency planning terms and concepts*
- 2** *Relate the contingency responsibilities of a GSS and its associated MAs*
- 3** *Use FSA's IT Contingency Planning Checklist*

The Department clarified the terms provided by NIST 800-34:

- **Continuity of Support Plan** – Intended to provide guidance for *short-term* service interruptions (less than 48 hours) that *do not require relocation* to an alternate processing site.
- **Disaster Recovery Plan** – Applies to major, usually catastrophic, events that deny access to the normal facility *for an extended period* (over 48 hours). The DRP focuses on long-term outages that *require relocation* to an alternate processing site.
- **IT Contingency Plan** – Not an actual documented plan, this term described the overall contingency planning process.

Boundaries and Scope

What should be included in a contingency plan?

- **Catastrophic failures**
- **System component failures**
 - Loss of server/switch/firewall...
- **Interconnecting systems**
- **Environmental impact**
 - Winter storm
 - Flooding
- **Failure of facilities**
 - Electricity
 - Water
 - Cooling



Contingency Planning Roles and Responsibilities

Contingency Planning requires the coordination of numerous individuals and teams. Some examples:

- **Contingency Planning Coordinator (CPC)** – manages the development and execution of contingency plan activities
- **System Security Officer (SSO)** – coordinates security activities and maintains contingency plan documentation
- **Damage Assessment Team** – determines the cause and extent of a disruption, and the estimated time for recovery
- **Recovery Teams** – conducts contingency measures to restore temporary IT processing capabilities; teams may include: **Databases, Servers, Applications** and **Alternate Sites**
- **Media Relations** – disseminates information to the public regarding an incident and FSA's responses
- **Legal Affairs** – coordinates all FSA legal responses
- **Physical/ Personnel Security** – protects physical assets and personnel during an emergency

NOTIFICATION/ACTIVATION

- Notification - Recovery Personnel are notified via call trees of a system disruption or emergency.
- Damage Assessment - The extent of damage and recovery time for the system is estimated.
- Plan Activation – The CPC determines whether to implement the plan.

“Houston, we have a problem.”
– Apollo 13

RECOVERY

- Temporary IT processing capabilities are executed in order to repair the damage to the original system and/or restore operational capabilities at the original or new facility.

“Sir, do we have a plan B?”

“Just out of curiosity: do we have a plan B?” – Titan AE

“I don’t know - I’m making this up as I go.” – Indiana Jones

RECONSTITUTION

- After the primary system is restored and tested, normal operations are transferred back to the organization's facility and recovery activities are terminated.

"All's well that ends well." –

Shakespeare

"Half of one, six dozen of the other."

– B. Fuller

Coordinating planning between GSS and MAs

n VDC

- **From where did the checklist come?**
- **What is on the checklist (basic info, FAQs, compliance requirements)?**
- **How is the list used?**
- **What does it mean to have a compliant contingency plan?**
 - No free toaster
 - No guarantee will recover
 - Required components exist
 - Framework for good contingency plan – likelihood for good plan goes up.