



DISASTER RECOVERY PLANNING





“It is a Dangerous World Out There, and information technology (IT) Leaders like Brain D. Voss (CIO Louisiana State University) know it.” Last Year’s headlines about calamities and breaches have put disaster recovery and Security at the top of IT agendas.”





PURPOSE

- Provide Background Information on Contingency Planning (CP)
- Describe how Disaster Recovery relates to Contingency Planning
- Plan Consideration
- Roles & Responsibilities
- Describe Disaster Recovery Services EPA offers
- Provide After Thoughts & Considerations



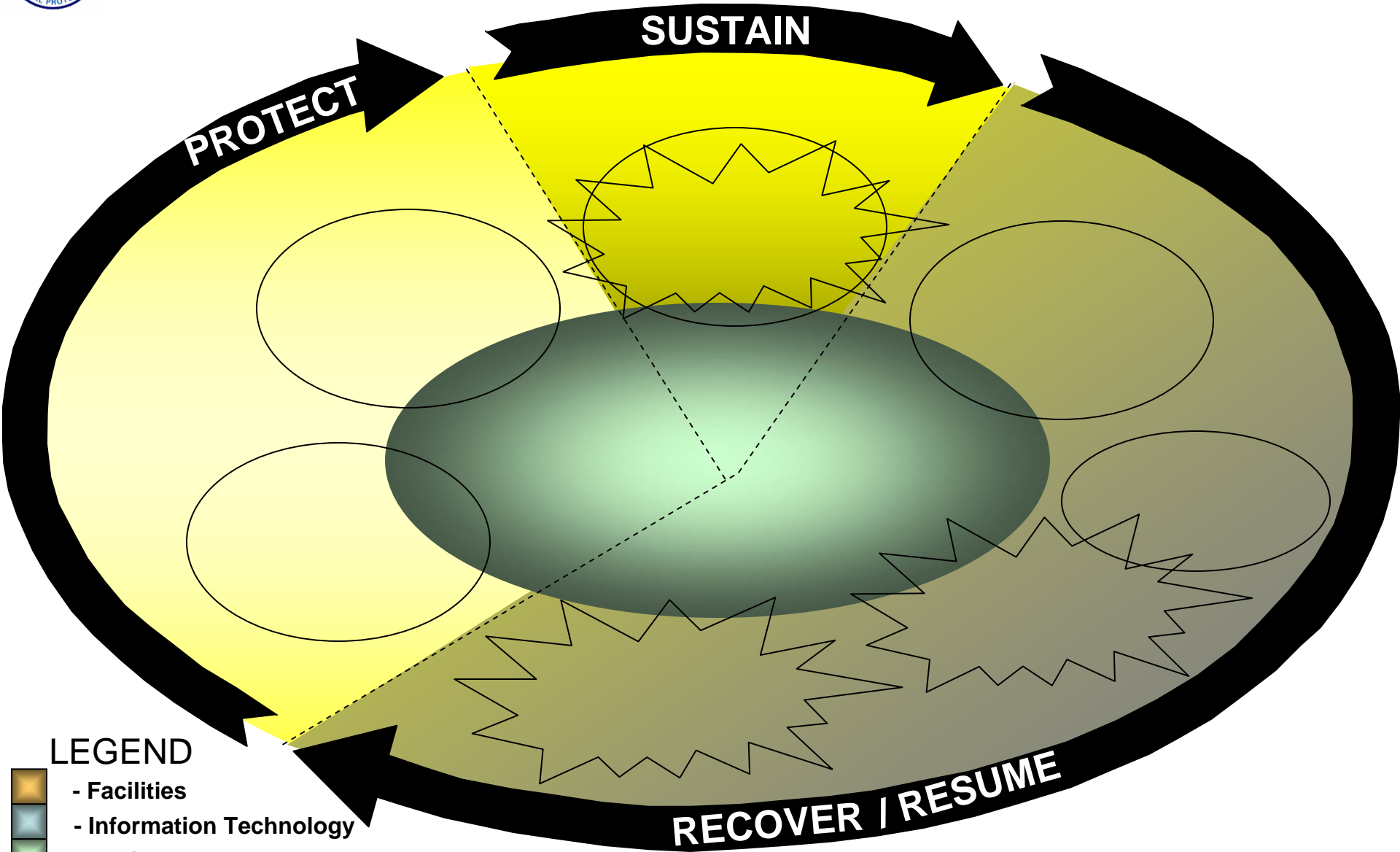


BACKGROUND

- Contingency Planning focuses on both the Business Processes within an organization and the associated IT Infrastructure that supports the capabilities to perform/provided services to the organization.
- Contingency Planning is very complex and massive. But, it can be broken down into 8 Component Parts that support the overarching design, i.e., each having a specific function.
- It is a form of Risk Mitigation that provides an organization with options for remediation.
- Contingency Planning will help to Recover/Reconstitute all or parts of the organization after experiencing an event which at some point renders the processes and/or IT infrastructure compromised.
- The portion of Contingency Planning that is implemented is designed to provide support for Short or Long Periods of time.



INTER-RELATIONSHIP OF DRP TO CP



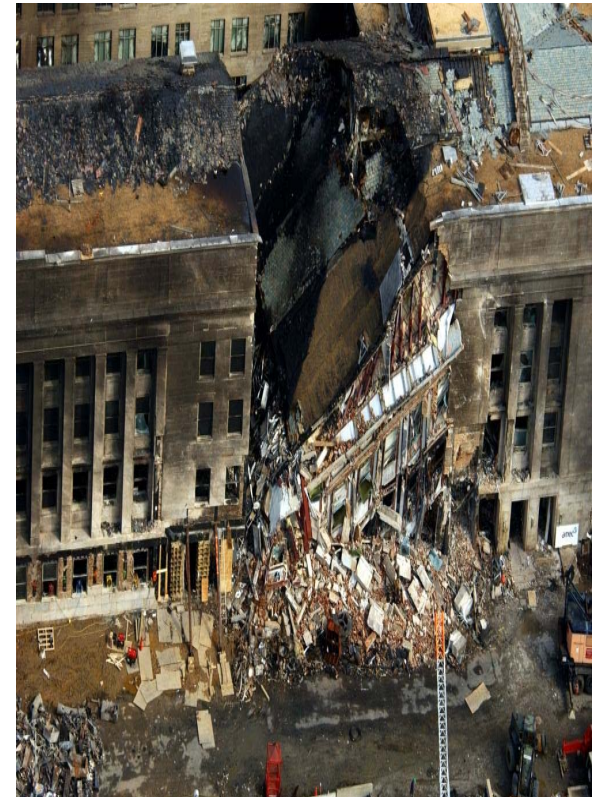
LEGEND

- Facilities
- Information Technology
- Business
- Major Impact



DISASTER RECOVERY PLAN (DRP)

- A DRP is a strategy for an organization to recover or resume operational capability
- They are IT focused but can support business processes
- They are driven by major events that deny access to normal facilities
- They are designed to support a need for an extended period of time (30+ Days)
- They provide restoration of operability at an alternate site after emergency occurs





SYSTEMS OWNER CONSIDERATIONS

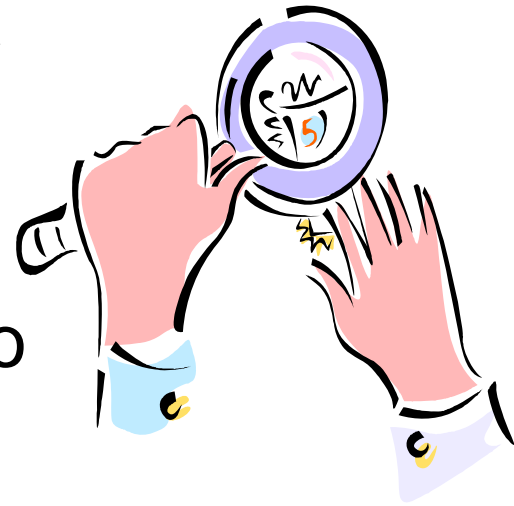
- All systems owners must develop a DRP for their applications, services, infrastructure, etc., which provides continual support to their lines of business and associated business partners.
- The system owner needs to understand the business and how technology can be used to provide support through difficult times.
- Systems owners need to assess, organize, develop, and coordinate their individual DRP with the “Lead Contingency Plan” organizer.
- System owners need to determine the roles and responsibilities within the plan for accountability purposes.
- Conduct a business impact analysis of the system, service, or application.





SYSTEMS OWNER CONSIDERATIONS

- Proponents need to identify the importance and criticality of system
- Determine amount of time the system can be down before experiencing major impacts to the lines of business
- Identify tools that can help develop a DRP and assess security concerns
- Consider the type of DRP that best supports the systems needs
- Balance the cost of a DRP solution to the associated performance metric when selecting a methodology to implement





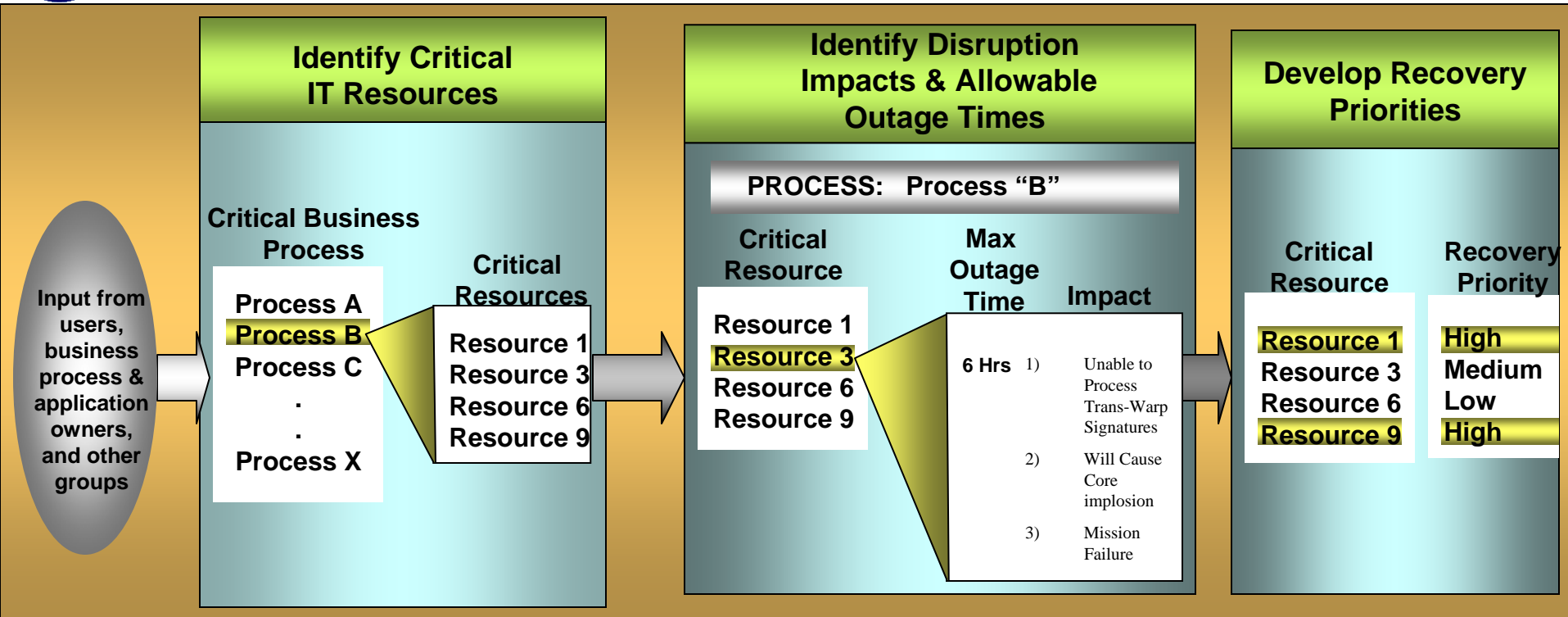
SEQUENCE OF EVENTS

- The DRP should include a sequence of events which annotates the time in which specific processes need to be brought back on-line.
- System owners need to identify and prioritize those processes that provide critical functionality to the business. This will help establish the order in which the processes or services are brought back “on–line”.
- System owners need to assess the impact of the event on the IT components to determine if items can be salvaged and used to support the implementation of the plan.





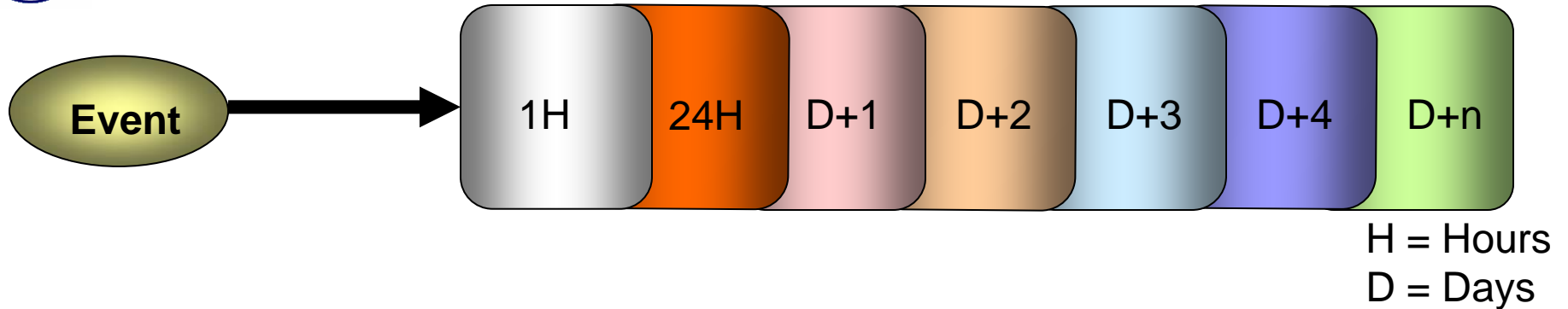
Business Impact Analysis



- The DRP should include a sequence of events which annotates the time in which specific processes need to be brought back on-line.
- System owners need to identify and prioritize those processes that provide critical functionality to the business. This will help establish the order in which the processes or services are brought back "on-line".
- System owners need to assess the impact of the event on the IT components to determine if items can be salvaged and used to support the implementation of the plan.



SEQUENCE OF EVENTS



- System owners need to identify steps or processes that will achieve different levels of operational capability within their DRP, ranging from “Minimal” to “Full” operational capability.
- System owners need to perform tests and a “Gap Analysis” of the DRP solution to verify the reality of the plan and continuously document the results in the plan
- System owners need to use feedback and “Lessons Learned” gained during test to strengthen their DRPs.








SITE CONSIDERATIONS

- System owners need identify a mile radius that the DRP alternate site should be implemented, i.e., by mile from site (200 – 500 miles) or by geographic region (West Coast Area)
- This helps to ensure that operational capability can be restored if the event impacts a specific location within the country.
- Owners need to determine if the location is accessible or too far to reach within timeframe specified in plan before minimal operational capability to required to be back “on-line”.
- Consideration needs to be given to the personnel required to travel to this site and perform the task needed to support the DRP. “Is it Realistic to reach and begin recovery procedures?” “Can the personnel perform the procedures?”



SITE TYPE

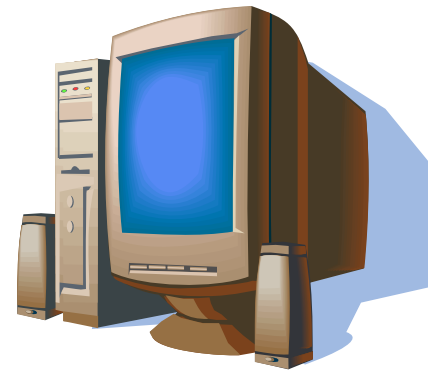
- Dependent on the technology selected, the following “Site Types” can support system owner’s processes for DRP.

	COST	DESCRIPTION
Cold		Site does not contain any IT equipment. Has plenty of space to implement DRP. May have power, telephone & environmental controls. Takes lots of time to bring site on-line. Low Cost
Warm		Site does contain some or all IT equipment to support system(s) relocation. Requires some time & preparation to complete operational status for systems. Medium Cost
Hot		Site contains the IT equipment to support system(s) relocation. Little time & preparation required to support transition. Staffed with personnel 24 x 7 hours per week. Medium to High Cost
Mobile		Not site dependent. Self-contained deployable units. Lengthy time to implement. Coordination required to configure unit. Requires vendor support and Service Level Agreements. Costly
Mirrored		Site contains all required IT equipment. Fully redundant with real-time information mirroring from original site. No time to establish. High availability and very expensive



TECHNOLOGY CONSIDERATIONS

- System owners should know that various types of technology are available to achieve implementation of the DRP.
- The type of technology used to achieve a DRP is dependent upon the requirements they define to support their business processes.
- System owners may define “high-end system availability” requirements, and then choose to “scale back” the technology chosen to implement the plan dependent upon cost restraints.





COST CONSIDERATIONS

- Cost to implement a DRP is dependent on the method and location chosen to support the plan.
- Cost may be shared or minimized if system owners have service level agreements in place with other organizations that require like functionality.
- Contractual and license issues for all IT equipment, services, and vendor support may impact cost and should be considered by the system owner.
- Cost may be effected by integration and interoperability issues with other IT solutions in their enterprise.
- Testing & training times needs to be included in the strategy and budget.
- Maintenance & life cycle replacement of all or parts of the IT components in the DRP need to be considered for budgetary purposes.





SECURITY CONSIDERATIONS

- System owners need to review the organization's security policies and controls.
- Perform a risk assessment and determine the level category (Low, Moderate, High) for the system and incorporate this information into the Security Plan. This can be done via ASSERT.

Threat or Vulnerability	Probability of Vulnerability Exploited	Potential Impact of Event		
		Confidentiality	Availability	Integrity
Fire	M	L	H	H
Hurricane	L	M	M	L
Hacker	H	H	H	H



SECURITY CONSIDERATIONS

- DRP should identify and prioritize security processes/protocols to ensure the integrity of system.
- Can be accomplished as part of the Business Impact Analysis

Resource	Recovery Priority
Resource "A"	M
Resource "B"	L
Resource "H"	H
Resource "X"	H



ACQUISITIONS CONSIDERATIONS

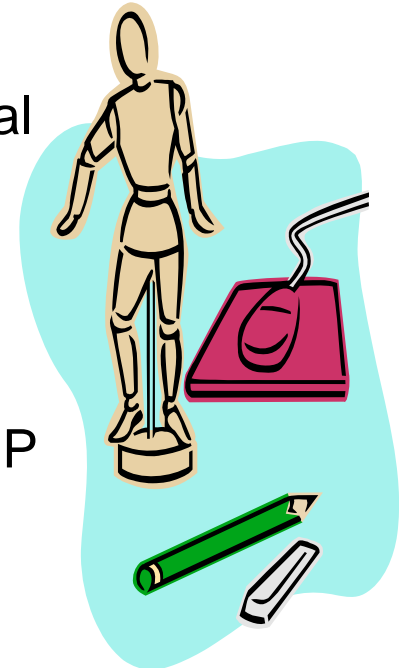
- Systems owners need to link the acquisitions of new software or hardware to the security plan and the DRP.
- Link to technology refreshes and life-cycle replacements.





ROLE & RESPONSIBILITY (SYSTEM OWNER)

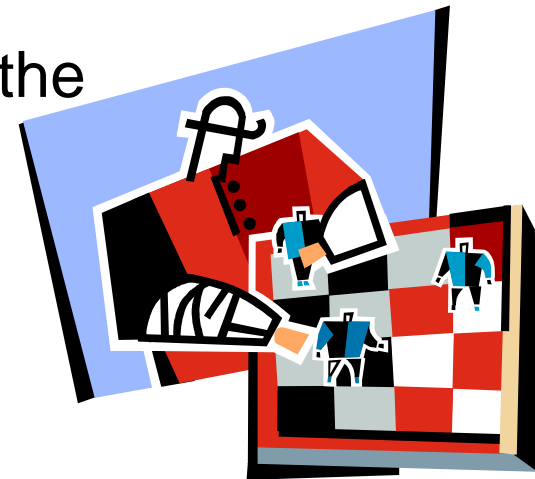
- Define what is to be accomplished, a timeline to complete the tasks, and the resources required to implement the plan
- Perform a business impact analysis and then identify the technology, tools, people, and skill-set available to them to project shortfalls in their plan to accomplished the recovery process
- Coordination and communication with other organizational units is essential to the development, testing, and implementation of the plan
- Break plan down into phases for implementation and assign task to specific groups, if required. “Be in the Know!”
- And, determine whether the process really requires a DRP





ROLE & RESPONSIBILITY (LEADERSHIP)

- Senior leadership needs to fully endorse and be very committed to supporting the need for a DRP.
- If the process is so critical to the organization, then funds need to be identified to support the recovery effort.
- Leadership needs to direct one individual to orchestrate the needs of all System owners and their DRPs for smooth transition and implementation. Otherwise, chaos can be the end result.





ROLES & RESPONSIBILITY (ORGANIZATIONAL)

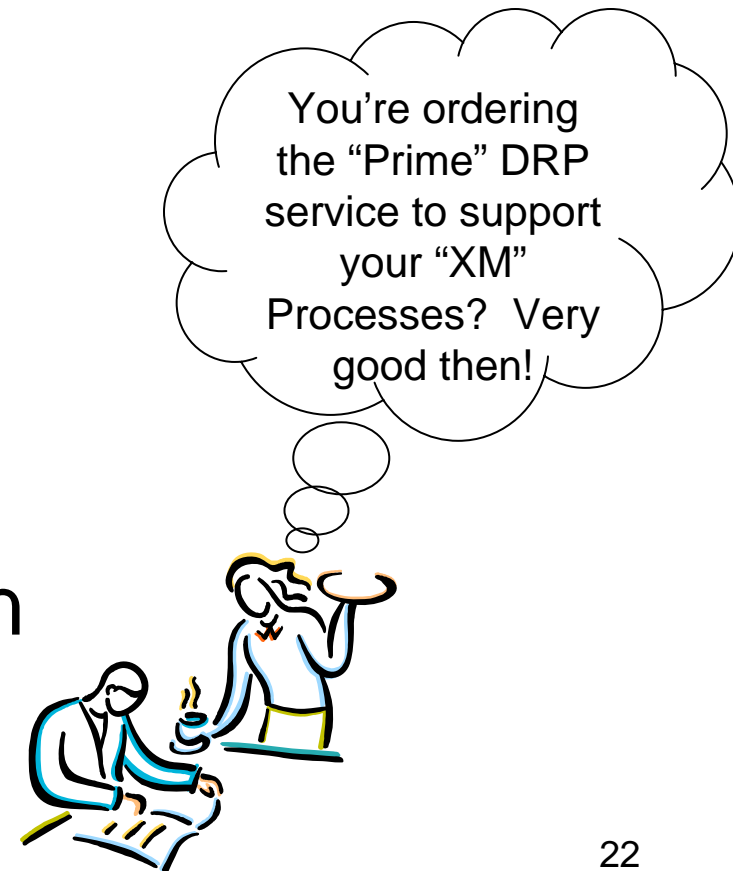
- Once the DRP is developed, how often does the organization test the plan to adapt to the external environment which influences this plan? Have the laws or business rules changed which may impact portions of the plan? And, is feedback captured during test and implementation to help modify the plan?
- If this is accomplished, then the DRP will be flexible enough to address the changes to the organization and be able to respond to anticipated events.





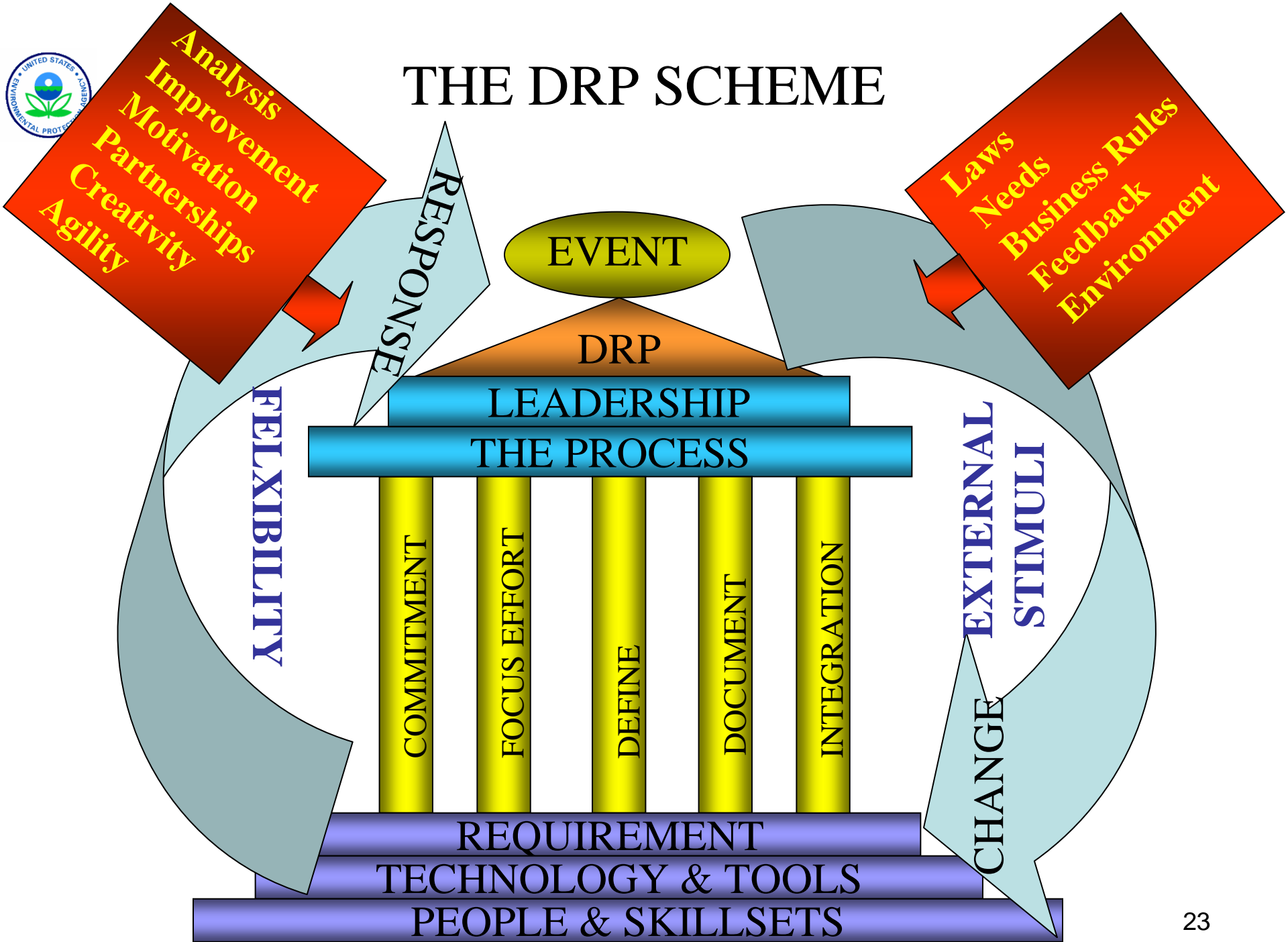
DRP SERVICES EPA OFFERS

- EPA does provide a DRP services as a fee for service.
- Currently, 7 major EPA systems subscribe to this service.
- [EPA's DRP Service](#) is provided by the National Computer Center located in North Carolina





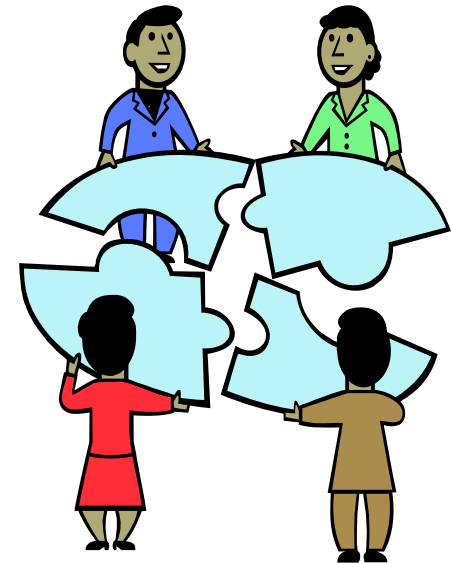
THE DRP SCHEME





“CONNECTING THE PIECES”

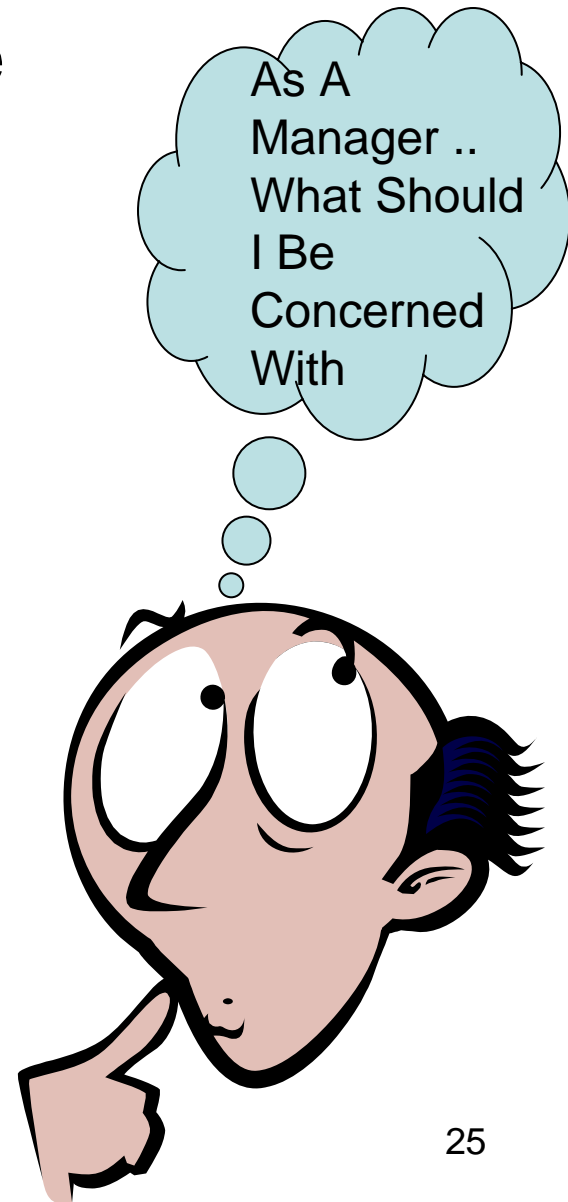
- Several DRPs may exist under one Contingency Plan
- Each DRP is tailored to provide options to react to different situations
- The system owner should perform A Business Impact Analysis to determine the effect the process has on the organization and associated lines of business
- DRP supports the Business Continuity Plan and can “piggy back” onto the COOP or IT Contingency Plan
- Leadership needs to be committed and stakeholders should be involved in the development of the plan
- Cost to develop a DRP is driven by technology and budget constraints
- Review [NIST 800-34](#) for guidance to develop plan





MANAGEMENT QUESTIONS

- How critical is the system or service in reference to costs associated to develop, test, and implement a DRP?
- Who is responsible to whom in the process and the level of involvement required to support it?
- Can a partnership be “forged” with another organization to support this need?
- Is there a DRP in place for my Critical Systems or applications?





QUESTIONS FOR SYSTEM OWNERS

- How critical is the system to the organization?
- What risk will be encountered if a DRP is not developed to support the system?
- Is there a DRP developed to support the process?
- Is the data backed-up and if so .. where is the data stored?
- What equipment is required to support a recovery process?
- Will there be any legal actions against the organization if a DRP is not developed for the process?
- Can a partnership with another agency be forged to support this requirement? If so, can the cost be shared with them?
- Where could an alternate site be established to support a DRP?
- How often should the plan be tested and when should the equipment be retired and “refreshed”?
- What funds are available to develop, test, and implement a DRP?
- Is feedback gathered from testing and implementation of the plan to enhance and make it better?
- How prepared is this system to address a catastrophic event?





ARE YOU PREPARED?