Disaster Recovery
&
Quality Assurance

Overview

- Disasters are happening more frequently and Recovery is taking on a different perspective.
  - Defining a Disaster/Disaster Recovery
  - Basic requirements in preparing for a disaster
  - The role of Quality Assurance in Disaster Recovery preparedness.
  - Identifying areas of concern in a GLP regulated environment

Regulatory Compliance

- Scope
  - Good Laboratory Practices (GLPs)
    - 21 CFR Part 58
      - Non-clinical laboratory studies
    - 21 CFR Part 11
      - Electronic Records and Signatures

Regulatory Expectation

- Role of Quality Assurance
  - Data integrity - Assurance that data is consistent and correct
    - Restorable
    - Accessible
    - Intact
    - Reconstructable

What is a Disaster??

- A disaster is the tragedy of a natural or human-made hazard (a hazard is a situation which poses a level of threat to life, health, property, or environment) that negatively affects society or environment. en.wikipedia.org/wiki/Disasters

Disasters

- Disasters of Today
  - Large scale
  - Small scale
  - Local
  - Global
- *Know what kinds of emergencies might affect your company both internally and externally*

What is Disaster Recovery??

- **Disaster Recovery** is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

http://en.wikipedia.org/wiki/Disaster_Recovery_Plan

What to Do?

- What will you do if your office building, plant or laboratory is **not** accessible?

- Put a plan in motion

Disaster Recovery Plan

- Disaster Recover Plan (DRP) is a detailed document that provides a roadmap to follow in order to restore (recover) your affected business services.
  - Laboratory
    - Equipment
  - Vivarium facilities
  - IT equipment &/or Infrastructure
    - Network
    - Telecommunications

Disaster Recovery Planning

- Components to Consider
  - Establishing a DRP committee
  - Defining what constitutes a Disaster
  - Performing the Recovery Risk Assessment
    - Business Impact Assessment
  - Identifying the types of systems to be recovered
  - Identifying the location of systems to be recovered
  - Determining recovery time targets
  - Using pre-existing processes
  - Defining the process for resuming business processes at the primary site.

Disaster Recovery Plan - Components to Consider

- DRP committee
  - Business Unit/System Owners such as supervisors, directors, managers, application administrators
  - Information Technology
  - **Quality Assurance Unit**

Role of Quality Assurance in DRP

- Advisory Role
  - Identify regulatory requirements
  - Establish quality standards
  - Consultation when preparing necessary documents

Disaster Recovery Plan Development

- Developmental Stage
  - Components to Consider (not limited to)
    - Personnel Roles & Responsibilities
      - **WHO ARE THESE INDIVIDUALS?**
    - Instructions for:
      - **Recovery**
      - Resumption
      - Plan maintenance
    - **Approval of Plan**

Disaster Recovery Plan Development

Role of QA

- Components to Consider…
  - **Recovery**
    - Ensure regulatory components are met
    - Quality is built in to the Recovery Process
    - Are test scripts written for each affected System?
    - Ensure the robustness of recovery test scripts
    - Ensure adequate documentation
      - Reconstructable events
  - **Approval of Plan**

Disaster Recovery Plan Testing

- Testing Stage
  - Components to Consider (not limited to)
    - Checklists
    - Walkthrough
    - **Disaster Simulation**
      - Testing and verification of technical solutions established for recovery operations
      - Ensure the ability to recover critical data in the event of a Disaster
      - Use of Test Scripts

Disaster Recovery Plan Testing

Role of QA

- Components to Consider…
  - **Disaster Simulation**
    - Ensure SOPs are in place
    - Monitor process as a phase inspection to ensure proper procedures are being performed according to the DRP.
    - Use of Test Scripts

Disaster Recovery Plan Maintenance

- Maintenance Stage
  - Components to Consider (not limited to)
    - **Training**
    - **Periodic Testing**

sting and verification of documented recovery
ocedures. A biannual or annual maintenance cycle
typical

Disaster Recovery Plan Maintenance

Role of QA

- Components to Consider…
  - **Training**
    - Documented evidence
    - **21 CFR Part 58**
    - **21 CFR Part 11**

Disaster Recovery Plan Maintenance

Role of QA

- Components to Consider…

  Periodic Testing

  - Are recovery & periodic testing procedures being conducted & complied with?
  - Is compliance supported by documented evidence?

What is “Event Documentation”?

- “Event documentation is the ‘silent’ GLP requirement because it is nowhere therein mentioned specifically and the reference to it is arcane. Clearly, Section 58.3(k) defines raw data essentially as the first record of an original observation but it was not without intent that the GLP drafters used the more comprehensive term "data" in Section 58.130, Conduct of a nonclinical laboratory study. This distinction was made to recognize the fact that laboratory experimentation results in a number of records that, strictly speaking do not fall under the definition of raw data.” *P. Lepore*

What is “Event Documentation”?

- To clarify: this is not RAW DATA but it is **DATA** and it needs to be maintained in order for study reconstruction
- Disaster Recovery Event

The 1st UNWRITTEN LAW

"IF IT ISN'T DOCUMENTED,
IT WASN'T DONE …"

Maintaining Compliance During a Disaster

- Compliance Stage
  - Components to Consider (not limited to)
    - **SOPs**
    - Post Disaster Operations
      - Lessons Learned
      - **Documentation Review**

Maintaining Compliance During a Disaster

Role of QA

- Components to Consider…
  - **SOPs**
    - Were DR SOPs followed?
      - Data security
      - Back-up procedures
      - Were the Software Life Cycle processes met
        - Change Control if needed
    - Criteria for assessing the disaster type
    - Criteria for assessing system impact

Maintaining Compliance During a Disaster

Role of QA

- Components to Consider…
  - Post Disaster Operations
    - **Documentation Review**
    - Does the DRP meet the regulatory requirements as appropriate for the business/service/system being restored?
      - Data integrity
    - Did you follow the DRP?
      - Data integrity
    - What software tools, techniques, and/or development methodologies are utilized?
    - Are processes in place to verify how the system can discern invalid/altered records?

Identifying Areas of Concern in a GLP Regulated Environment

- Were records maintained off-site and subsequently retrieved?
- Is there a Recovery Co-location site?
  - If so, has a vendor audit been conducted
  - If so, what SOPS or formal procedures do they follow in the event of a Disaster
- Are all back-up systems identified according to the system configuration logs?
- What procedures do the Labs use in the event systems even equipment are unavailable?
  - What's the process after the system has been restored

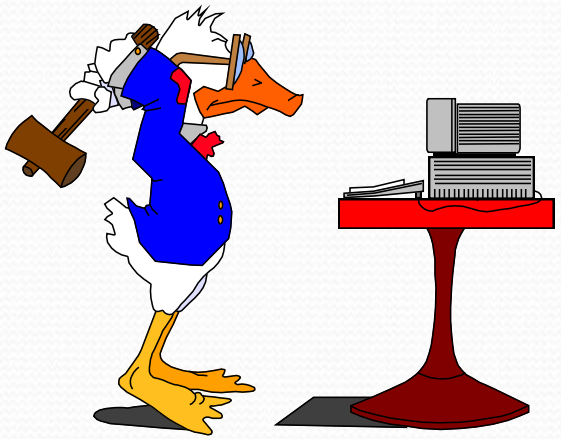
Identifying Areas of Concern in a GLP Regulated Environment

- Vendor Assessment
  - Off-site archive location (Paper vs Electronic Data Archives)
  - Specialized assay, water analysis, analytical chemistry
- What are the Disaster Recovery procedures for vendors that provide subcontracted data collection or data record retention?
  - What happens to your data in the event of a Disaster?

Are You Prepared?

- QA inspections are essential
  - Verify the existence of objective evidence
  - Assess how successfully processes have been implemented
  - Ensure GLP compliance has been maintained
  - Promote continuous improvement

FDA Citation



- Failure to back-up data with subsequent loss due to hardware failure

- Recovery in a different light
  - Customized to fit the specific disaster/disruption
  - Provides evidence that the system is doing what it is supposed to do & will continue to do so in the future

Any Questions?

Cynthia L. Smith, RQAP-GLP
Quality Specialist III

RESOURCES

- Emergency Preparedness and Business Continuity Standard (NFPA 1600) developed by the National Fire Protection Association and endorsed by the American National Standards Institute and the Department of Homeland Security.
- http://en.wikipedia.org/wiki/Disaster_Recovery_Plan
- http://www.ready.gov/business
- Red Apple II, 2008
- Association of Records Managers and Administrators (ARMA) www.arma.org