FFIEC Guidelines:
As of July 2013, we are unaware of any specific guidelines issued by the FFIEC and/or individual regulatory bodies (such as the FDIC or OCC) related to testing incident response plans. The following is based on FFIEC guidelines for testing a financial institution's Business Continuity Plan (or Disaster Recovery Plan).

- **Audit:** Independent review of the Incident Response Plan (IRP). Purpose is to ensure plan is appropriate, complete, and current. Ensures compliance with FFIEC regulations. Also tests for awareness on the part of all appropriate personnel (Board, Management, BCT, Employees, and Partners). Reports deficiencies in a risk-based format. Only high and critical risk deficiencies are reported beyond the BC Team.
- **Tabletop Exercise / Structured Walkthrough:** A walk-through is the most basic type of test. Its primary objective is to ensure that critical personnel from all areas are familiar with the IRP. It is characterized by:
    - Discussion about the IRP in a conference room or small group setting;
    - Individual and team training; Confirmation of information in calling trees, vendor trees, etc. and
    - Clarification and highlighting of critical plan elements.
- **Walkthrough Drill / Simulation Test:** A tabletop test is somewhat more involved than a walk-through because the participants choose a specific event scenario and apply the IRP to it. It includes:
    - Practice and validation of specific functional response capability based on specific scenarios;
    - Focus on demonstration of knowledge and skills, as well as team interaction and decision-making capability;
    - Role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment;
    - Mobilization of all or some of the crisis management/response team to practice proper coordination; and
    - Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan.
- **Functional Drill / Parallel Test:** Functional testing is the first type that involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the IRP. It includes:
    - Temporarily suspending, or simulating suspension of, critical systems.
    - Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning;
    - Actual or simulated response to alternate locations or facilities using actual communications capabilities;
    - Mobilization of personnel and resources at varied geographical sites; and
    - Varying degrees of actual, as opposed to simulated, notification and resource mobilization.
- **Full Interruption / Full-scale Test:** Full-scale testing is the most comprehensive type of test in a disaster recovery plan. We do not believe that this type of testing should translate over to an incident response test, because (unlike disaster recovery) we would not want to create an incident in order to test our response to it.
- **Maalox Testing:** *(Note: Maalox is an over-the-counter antacid product.)* This is a nonofficial term infotex uses to describe those disaster recovery tests that are actual live incidents. In other words, the response to an audit question is "well, we tested our plan when the xyz system went down." Though this type of test is not addressed in the FFIEC guidelines, over time, a general interpretation of most auditors has evolved that organizations using actual events to count as a test can been sufficient as long as:
    1. Your examiner agrees with the concept;
    2. A post-mortem review is conducted with action items and plan updates;
    3. The actual event was a scenario in your existing plan; and
    4. The actual event is not a scenario type that has already been tested in your overall test plan.