


Microsoft
Over 400 new features. They're everywhere.
The difference is obvious.

Microsoft
Visual Studio 2005

Play the game now and see what's new 

FDIC compliance and disaster recovery

March 6, 2006

Takeaway:

If you are an IT professional for a member institution of the FDIC, there are some pretty stringent guidelines for disaster recovery preparation. Make sure you know the questions auditors will be asking when it's your turn to be grilled.

Rounding out our discussions of regulatory compliance and disaster recovery (DR), we'll take a look this week at the Federal Deposit Insurance Corporation ([FDIC](#)) and what regulations it sets forth for banks and similar financial institutions when it comes to DR planning.

The FDIC is a government agency responsible for the oversight of banking and lending institutions to ensure that in the event of a crisis, depositors' monies can be returned to them on demand. Essentially, this means that if all else fails, the FDIC will insure each depositor for up to a specified amount of cash—the amount posted at the bank and in all contracts and other written instruments. Until recently, the FDIC has been very lax on even offering guidance on DR for member institutions, but it has changed its tune considerably.

[Current regulations](#) still maintain that DR plans must be in place and functional before insurance can be issued, and it must be proven to remain intact in order for each FDIC audit to be passed. However, the criteria for what will make a successful DR plan has become much more involved over the past several years.

For example, [FDIC examinations](#) now routinely question bank employees about what solutions are in place for backup and recovery of sensitive data—such as account information. They also grill management about what technology has changed since the last audit, how the board of directors has been kept up-to-date on this technology, and how it will be protected. All of this means that your role as an IT worker becomes a lot more visible, since management must answer these questions. Here are the primary questions you will be asked regarding DR by an FDIC auditor, according to the FDIC's "[Information Technology Examination Officer's Questionnaire:](#)"

Tips in your inbox

How well can your organization deal with an emergency? The Disaster Recovery newsletter helps you protect your valuable data.

[Automatically sign up today!](#)

- Do you have an organization-wide disaster recovery and business continuity program (Y/N)? If yes, please provide the name of your coordinator:
- Are disaster recovery and business continuity plans based upon a business impact analyses (Y/N)? If yes, do the plans identify recovery and processing priorities (Y/N)?
- Is disaster recovery and business continuity included in your risk assessment (Y/N)?
- Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations (Y/N)?
- Do business continuity plans address procedures and priorities for returning to permanent and normal operations (Y/N)?
- Do you maintain offsite backups of critical information (Y/N)? If yes, is the process formally documented and audited (Y/N)?
- Do you have procedures for testing backup media at an offsite location (Y/N)?
- Have disaster recovery/business continuity plans been tested (Y/N)? If yes, please identify the system(s) tested, the corresponding test date, and the date reported to the Board.

IT security is also scrutinized during your regulatory audits. FDIC examiners are instructed to ask about access control for data systems and the security protocols that you have in place at the physical plant and across the network; in addition, auditors may demand an

outline of your network topology for review. This means that you're going to be working very closely with compliance officers from your company in order to provide this information and interpret the results.

The FDIC only regulates banking and similar institutions, but the lessons learned from these regulations can offer a firm base for DR planning in many other fields. Even if you don't have an FDIC auditor banging on your door, the questions they ask can be a very valid aid in securing your own organization.

To see the other recent articles on DR and compliance, check out the [Disaster Recovery archive](#) page.

White Papers

- [Integrating Compliance Into Your Disaster Recovery Plan](#)
- [Webcast: File System Replication for Data Protection Solutions](#)
- [Webcast: The Secure Remote Access Imperative for Healthcare](#)
- [IBM provides critical aid to tsunami victims in southern Asia](#)
- [Beyond disaster recovery: Becoming a resilient business](#)

Additional Resources

[Tech Toolshed](#)

<http://www.techtoolshed.com>

[Learning CD-Roms](#)

<http://fasttrack.techrepublic.com>

[Quick Reference Charts](#)

<http://quickref.techrepublic.com>

[TechRepublic's Catalog](#)

<http://www.techrepublic.com/catalog>

[Copyright](#) ©1995- 2006 CNET Networks, Inc. All Rights Reserved.
Visit us at www.TechRepublic.com