The Risks Associated with Reciprocal Agreements

FFIEC Definition of a Reciprocal Agreement

"An agreement whereby two organizations with similar computer systems agree to provide computer processing time for the other in the event one of the systems is rendered inoperable. Processing time may be provided on a "best effort" or as time available" basis; therefore, reciprocal agreements are not usually acceptable as a primary recovery option.

If the facilities are not geographically distributed in different locations, an area-wide disaster could render both of the sites useless. In addition, this type of facility could be more difficult to manage and administer. Management should also understand that implementing a reciprocal agreement might not always provide an optimal back-up solution due to limited excess capacity.

In most cases, reciprocal agreements are unacceptable because the institution agreeing to provide back-up has insufficient excess capacity to enable the affected institution to process its transactions in a timely manner. If an institution chooses to enter into a reciprocal agreement and can establish that such an arrangement will provide an acceptable level of back-up, the agencies expect such an agreement to be in writing and to obligate each institution to make available sufficient processing capacity and time. The agreement should also specify that each institution would be notified if the other institution implements equipment and software changes, and provisions should be included addressing each institution's right to conduct annual tests at the reciprocal site."

Assessing the Risk

Your Business Resumption Plan must mitigate the following risks:

- Reputation Risk
- Compliance Risk
- Transaction Risk
- Financial Risk

Things to consider before signing Reciprocal Agreements

1. How long will it take you to recover your critical functions at the reciprocal bank?
2. Do you and the reciprocal bank use the same core banking vendor and applications?
3. If a disaster did strike and you move to a reciprocal bank, what impact would this have to your reputation? Is there a possibility that you would lose clients, growth and profits?
4. How long will the reciprocal bank allow you to operate in their facility?
5. How long will it take for your core provider to install a new communication circuit into the reciprocal bank to gain access your data? You cannot mix your customer transactions with the reciprocal bank's transactions using the existing communication circuit as this is a GLBA violation. The two communication circuits must be segmented to protect confidential information from being shared between the two banks.

6. How long will it take to install and configure a telephone system at the reciprocal bank? Incoming phone calls should not be mixed with the reciprocal bank's incoming calls.
7. Does the reciprocal bank have spare PC's, file servers, and other critical hardware that can be immediately used to restore your back-up systems? You cannot restore your data onto the reciprocal banks file servers as both system administers would have access to each other customer confidential information. This is a GLBA violation.
8. How long will it take you to purchase, install and configure new computer hardware within the reciprocal bank space? Do they have adequate space?
9. How would digital video security be configured in the assigned space at the reciprocal bank that would be specific for your bank and your customers? How long will it take to order and install new video surveillance equipment?
10. Does the IT infrastructure within the reciprocal bank support the rapid addition of voice and data circuits?
11. Does the facility infrastructure within the reciprocal bank support additional servers (e.g., Power, phone/data cabling, UPS, HVAC, fire detection & suppression systems, secure server room space, etc.)?
12. Does the reciprocal bank have sufficient extra space where you can securely perform critical functions? For example:
    a. Teller Windows
    b. Drive up Windows
    c. New Accounts Desks
    d. Loan Officer Desks
    e. Deposit and Loan Operations Departments
    f. Secure Wire Transfer Room
13. Does the reciprocal bank use the same critical banking printers? Do they have sufficient spare equipment that can be made available to your employees? For example:
    a. Teller Receipt and Validation Printers
    b. Check Image Scanners
    c. Flatbed Scanners for Document Imaging
    d. Signature Card Scanners for Signature Retrieval Systems
14. Does the reciprocal bank have a spare cash vault that can be used for your teller drawers? If not, do they have open cash drawers with spare keys that can be assigned to your employees?
15. Does the reciprocal bank have a spare document vault where salvaged bank records can be relocated and securely stored?
16. Would night deposit services be available to your customers? Have procedures been developed to safeguard both banks deposits?
17. How would you retain customers, attract new customers and continue to sell products and services inside your competitor's bank facility? The problem is your customers will now have access to the following reciprocal bank competitive information:
    a. Rates
    b. Deposit and Loan Products
    c. Pricing and Fees
18. How far is the reciprocal bank from your bank?
    a. Too close, the disaster may impact this bank as well.
    b. Too far, your customers may not want to travel to the new location.

19. Has vendor due diligence been performed for this institution per your Vendor Management Policy?
20. What are the reciprocal bank's physical and logical security procedures? Are they consistent with your standards?
    a. Physical Security Policy
    b. Information Security Policy
    c. Remote Access Policy
    d. Vendor Management Policy (especially on-site vendor procedures)
    e. Record Retention and Secure Destruction Policy
    f. Network Security Policy/Standards
    g. Hiring Practices
21. Is the reciprocal bank's business continuity plan strong enough to withstand a disaster while you are located in their facility? How would a new disaster impact your banking operations and reputation?
    a. When did they last perform a disaster recovery test?
    b. Do you review their test results annually?
    c. Are their procedures consistent with your requirements and Business Continuity Policy?
22. Is your bank prepared to provide the infrastructure, space, equipment and security to the reciprocal bank if they declare a disaster?
    a. Where will employees from the reciprocal bank be working in your facility?
    b. How will this impact your customer service, retention and growth?
    c. How long are you prepared to allow the reciprocal bank to operate in your facility?

Contact us today and learn how Recovery Solutions Mobile Bank Facilities and technologies fully mitigate your business resumption risks.

Recovery Solutions

12207 Rhea Drive
Plainfield, IL 60585
815-577-1999

www.recoverysolutions.com