

How to Use This Manual

Recent developments in the banking industry have made the need for clear, well-planned data processing (DP) policies and procedures more urgent than ever. Bank examiners are pushing hard for banks to adopt DP policies and procedures to help minimize the risks banks are exposed to in this area. Every area of data processing is under scrutiny by the examiners, and the overriding concern is that since data processing is at the heart of bank operations, the only way to assure continuing security and operations of a bank is to make sure it has a complete set of board-approved policies and procedures in place. To help you deal with the challenge of developing and maintaining comprehensive, yet practical, DP policies and procedures, we have concentrated on making this a “how to” guide that will lead you through every aspect of the review and development process. In addition, we have developed a complete set of sample DP policies and procedures covering every major DP operating area. You can adopt these policies and procedures “as is,” or you can modify them to suit your bank’s particular needs in this area.

Bank Data Processing Policies and Procedures has been structured to meet the needs of different users — from policy developers to those supervising or evaluating the work of others. Policy developers will find that this manual will help them to organize their approach to data processing policy and to ensure that specific areas are covered and analyzed during the policy development process. In addition, this manual will help in reviewing the effectiveness and adequacy of your DP policies — whether you are testing to see if a particular area is covered by a policy, determining whether a policy contains the information required, assessing the scope of a policy, or ensuring that a policy meets the requirements of regulatory examiners.

In a 2006 Community Bank Technology Survey undertaken by Independent Community Bankers of America, BKD, LLP, CPAs, and Advisors, and Plante Moran, 83 percent noted that their organization had an Internet banking site that allowed customers to perform Internet banking transactions. The functions most frequently offered through the Web sites included:

- Pay bills electronically
- Update account information
- View check images
- Apply for loans
- Apply for credit cards

The survey also noted that security is a primary focus area with the majority of respondents having specific policies to address the following focus areas:

- Acceptable Internet usage/security
- IT Disaster Recovery and Business Continuity Plans
- Data Security
- Data Security breaches
- Service Provider Selection

Of the survey respondents, 47 percent outsourced security monitoring to another company. Approximately 69 percent had an external systems/network security assessment and approximately 58 percent had an internal systems/network security assessment.

Changes in the financial services industry, and therefore, the regulatory assessment of management supervision, have become critical issues for every bank. The DP area is no exception. Examiners are reviewing DP policies and procedures more closely than ever before; in turn, bank directors are being encouraged to ask the hard question, “What is our bank’s policy regarding this operation, product, or service?” *Bank Data Processing Policies and Procedures* is a resource designed to help bank management in:

- Assessing DP policy needs
- Evaluating whether current DP policies meet compliance standards
- Planning and developing new DP policies and procedures as required

For years, there was talk of a checkless society; 2003 brought a new first to the banking industry. For the first time, electronic payments surpassed cash and checks as the consumers preferred form of payment for in-store purchases. Decreasing check volume presents an enormous growth opportunity for electronic payments. The Federal Reserve Board approved revisions/amendments to Regulation CC to implement the Check 21 Act which became effective October 28, 2004. Check 21 authorized a new negotiable instrument called a substitute check and provides that a properly prepared substitute check is the legal equivalent of the original check for processing purposes. A substitute check, therefore, is a reproduction of the original check that meets specific legal requirements and can be processed like a check. While checks are clearly a part of the financial services system, the movement of funds is edging closer to a paperless check environment.

THE POLICY DEVELOPMENT PROCESS

The first section of this manual provides an overview of the entire DP policy development process. It describes in detail:

- Why you need DP policies
- Where to begin in developing and modifying DP policies
- What should be included in DP policy statements
- How to write an effective DP policy
- What regulatory agencies expect with respect to written DP policies
- How to implement and maintain a DP policy

SAMPLE DATA PROCESSING POLICIES

Sample DP policies are provided for your reference in the policies section of this manual.

Each DP policy consists of four parts:

1. An introductory outline that summarizes the policy’s focus area, regulatory risks that the policy protects against, major policy elements, and other considerations
2. A heading on each policy page that provides identification information
 - Attribution to a specific functional area within the bank
 - Date when the board adopted the policy
 - Date when the policy was last reviewed

- The individual or department responsible for maintaining the policy
3. The sample policy itself, prepared according to the basic format provided in the detailed discussion of the policy development process
 4. A regulatory compliance checklist to be used in evaluating whether new or existing DP policies meet compliance standards

These sample DP policies were not designed to fit the needs of every bank, nor could they ever be written to serve this purpose. Rather, banks or bank holding companies should use these sample DP policies as a starting point and then tailor the policies to meet their own specific organizational needs.

MULTI-FACTOR AUTHENTICATION

The federal regulatory agencies require each financial institution to have multi-factor authentication processes and controls in place for their e-banking programs. Institutions should work closely with their primary data processing service providers to have a multi-factor software security program that encompasses the following types of controls:

- Layered security levels reflecting different risk ratings assigned by the institution and/or customer, utilizing different authentication techniques, e.g., response to phrase, date, picture, unique identifier, or other type of question.
- Registration of customer PC location

In addition, institutions should utilize multi-level tokens. This approach facilitates access by the designated individual from different PCs. Implementing a security software package for customer e-banking access, e.g., the software security program incorporates multi-factor authentication solution and also facilitates multi-level security for customers.

Regarding informing customers, the following are common techniques utilized to advise account holders of enhanced security procedures:

- E-mail communication
- Web site notice
- Statement stuffers
- Personalized letters and/or mailings, e.g., by name and specific account relationship
- Web site training video

In several instances, management team member point out that in preparing and implementing the multi-factor authentication controls, a major review was undertaken of internal policies and procedures. These reviews served as a process to further enhance internal controls and procedures and therefore, management commented there were ancillary benefits to the review.

EMERGING ISSUES

Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers

The processing of cross-border wire transfers frequently involves several financial institutions. In addition to the originator's bank and the beneficiary's bank, other banks often are involved. There are circumstances where one or more of these cover intermediary banks is located in a jurisdiction other than the jurisdictions where the bank

of the originator and the bank of the beneficiary are located. Consequently, cover payments are necessary. Cover payments are used by a bank to facilitate funds transfers on behalf of a customer to a beneficiary, most often in another country, but also in the same country when a foreign currency is used.

Currently, existing messaging practices do not ensure full transparency for the cover intermediary banks on the transfers they facilitate. Transparency is limited when the message format used to settle the interbank payment does not contain information about the originators and beneficiaries. Lack of originator and beneficiary information for funds transfers can hinder or limit a cover intermediary bank's ability to accurately assess risks associated with correspondent and clearing operations. As such, more detailed information regarding originators and beneficiaries of funds transfers can improve compliance with locally applicable requirements (such as the blocking, rejecting, or freezing of assets of designated individuals or entities and monitoring for suspicious activity) and enhance a bank's risk management processes with respect to funds transfers.

Supervisors must be satisfied that banks develop and implement appropriate policies, procedures, and processes to address respective capacities as originator banks, intermediary banks in the cover payments chain, and beneficiary banks. Supervisors may take several steps to assess their supervised institutions risk management practices with respect to cover payments. Supervisors should carefully review the risk management practices relating to those operations. Supervisors should be satisfied that appropriate internal controls are in place to monitor wire transfer activity, that these controls are effective, and that banks are in compliance with supervisory and regulatory guidance.

APPENDIXES

Finally, the appendixes to this manual include several checklists and forms that will assist you in the planning process. Appendix A includes policy implementation worksheets.

The remaining appendixes present information issued by various regulatory authorities that pertains to specific bank policies or procedures. A quick reference guide to recent regulatory issuances is to be kept in your manual, and all issuances related to data processing are stored on your CD.

GLOSSARY

The glossary in your manual contains definitions of words and acronyms that will help you better understand the information in this manual.

YOUR COMPANION CD

As part of your purchase of *Bank Data Processing Policies and Procedures* you receive a companion CD. This disc contains all of the information in your print manual that shows you how to make sure your policies and procedures are being followed and accomplishing what they were intended to do.

Insert your CD into your desktop computer, and the autoplay feature will assist you in navigating the files. You can search quickly and easily for specific guidance and policies.

Customize Your Policies

From accounting for software costs to vendor management, the CD contains sample policies for every key area of data processing. Checklists, examples of documentation, and clear guidelines can be used for your own policies for your operation.

You can easily customize the documents on the CD using Microsoft Word so that you keep your IT functions current with the latest compliance issues. Sample policies are provided for each key area that you can easily adapt to your specific requirements.