Guidelines for Internet Based Application Controls

The electronic delivery of services over the Internet has proven to be both popular and cost effective. It is expected that the volume of business, number of users, and the variety of functions delivered via this technology will continue to increase. As the number and sensitivity of transactions increases, it is imperative that the associated risks are managed with adequate internal controls.

Internet delivery of services is replacing manual and process driven delivery methods. The controls and procedures that are in place for the older systems are generally not effective in controlling and providing oversight of an automated Web based system. Most controls in manual systems were typically designed for interaction between staff members of the credit union and their respective corporate. Web based systems are rapidly removing that interaction. Authentication procedures for critical transactions are integrated into the software. Sensitive transactions are being confirmed at the credit union rather than through a corporate initiated verification process. For example, in many systems wire transfers are confirmed within the credit union rather than by the corporate staff back to the credit union.

Many control features originally in place at the corporate are being shifted to the member credit union. Some systems delegate system administration to the natural person credit unions to facilitate member services. Delegation of administrative responsibilities to the credit union may be a practical and convenient approach to facilitating services. However, along with this delegation, systems should provide credit union management with the tools to ensure proper administrative use. A well-designed control system gives the corporate reasonable assurance that it is receiving authenticated, non-repudiated transactions. Controls also empower the natural person credit union with the ability to manage oversight of the system, ensure proper use, and direct administrative activity.

New technology also offers the opportunity to facilitate the internal control process with improved security and state of the art reporting systems. The technology exists and is in place in some systems, to pro-actively notify management of the occurrence of critical administrative activities or system anomalies. For example, if a new administrative account is created or there are changes in administrative authorities for an existing account, appropriate staff members are automatically notified without having to wait for a month-end report. The notification can be provided via e-mail or a report delivered over the Internet.

Additionally, management reporting tools can zero in on specific functions that merit review. Alternatively, ad hoc reports can be developed to suit specific management needs. With these capabilities, managers can focus on critical events and not have to perform exhaustive reviews of voluminous reports as part of the oversight process.

The implementation of system controls will vary depending on the risk involved and the nature of compensating controls in the corporate. The purpose of this guidance is to advise corporate management of OCCU’s expectations for security when these systems are reviewed during examinations or supervision contacts.

The corporate should address, at minimum, the risk areas noted below:

1. Agreement - The agreement covering this type of processing should clearly delineate the responsibility of the corporate and the natural person credit union with respect to security, unauthorized use, and unauthorized transactions.

2. Audit Trails - It is vital that Internet based systems provide an adequate audit trail of critical system activities. At minimum, audit trails should include all activity performed by administrators, account lockouts, file maintenance, user account maintenance, and records of transactions.

3. Authentication - Procedures should be in place to ensure that users accessing the system have been authorized by credit union management to do so. Primary methods of user authentication such as digital certificates, challenge/response phrases or alternative verification of users for critical transactions are strongly encouraged.

4. Management oversight - Credit union management approval should accompany requests to add users to the system for authorities that permit sensitive transactions.

5. Management reporting - An adequate management reporting system that facilitates the review of critical activities by management.

6. Enforcement of strong passwords - System software should prohibit utilization of weak or ineffective passwords. Passwords and PINs, as appropriate, should be changed on a regular basis.

7. Inactive accounts - Accounts with no or infrequent activity should be deactivated and only reactivated on written request.

8. Control administrative activities

a. Ensure that the number of system administrators is kept to a minimum.

b. Provide for adequate oversight of administrative activities.

i. Activities of administrators having to do with critical user authorities should have dual control features that requires management approval before it is fully enabled. For example, a manager would be required to perform an approval function that would verify the authority for wire transfers

ii. Systems should provide for automatic notifications to appropriate management when administrators change user authorities, add or delete users or assign critical functions. Responsible managers should receive notification of critical administrative activities as they occur.

9. Monitor the system - Systems should have the facility to monitor and alert management of failed access attempts, attempts to access files without proper authority, transactions that appear to be anomalies (for example, wire requests for large dollar amounts), attempts to exceed established dollar limits, large volumes of similar transactions or otherwise unusual requests.

10. Provide adequate management reports - Reporting systems should be available that provide credit union management the tools to review:

a. Administrative activity;
b. Records of transactions;
c. File maintenance activities; and
d. Security violations.

A well-designed security and administration system is a critical component of system development. It facilitates management and expansion of services. Sound system controls add a high degree of creditability to Internet initiatives. They enable a corporate's natural person credit union members to provide better service to their members and assure reasonable management oversight. Appropriate controls provide an intrinsic quality to the corporate service and helps ensure the integrity of the credit union system.

bcc: Reading File
Regional Directors
All OCCU Staff
Office of General Counsel
Office of Examination and Insurance

draft: S:\WorkIn Process\Office Staff\shetler\Application Control Guidelines Letter.doc

final: S:\Directives\OCCUGuidanceLetter\2001-04-Application Control Guidelines.doc