

Internet Banking Audit Program

The objectives of this audit are:

1. To gain an understanding of the bank's Internet Banking product line, transaction flow, and settlement processes.
2. To ensure that adequate internal controls are in place to minimize errors, discourage fraud, and provide an adequate audit trail.
3. To determine whether the board of directors has adopted effective policies for Internet banking and these policies and procedures are being followed.
4. To determine if contingency and disaster plans are adequate.
5. To determine if the bank complies with applicable regulations.
6. To determine whether management has instituted controls that are appropriate to the type and level of risks arising from Internet banking.

Preliminary Procedures

1. Obtain a current list of the personnel who work in the Internet Banking Department, including their duties.
2. Obtain or prepare a flow chart and/or narrative detailing the Internet Banking system.
3. Obtain the following documentation prior to the audit:
 - Summaries of strategic plans. OCC
 - Independent reviews, assessments, or system certifications performed by consultants or technology experts contracted by the bank. (Note any outstanding deficiencies.) OCC
 - Information detailing Internet Banking activities conducted. FDIC
 - Details regarding complaints specific to Internet Banking. FDIC
 - External audit reports and related materials. FDIC
 - Summaries of relevant operating policies and procedures. FDIC
4. Determine whether external vendors are used and what services or products are provided. Document who is responsible for development, operation, and/or support of the Internet banking system. OCC
5. Review documentation and conduct discussions with management to determine:
 - How security for Internet banking is addressed.
 - How management supervises Internet banking functions, including outsourced functions.
 - Any significant changes in policies, practices, personnel, or control systems.
 - Any internal or external factors that could affect the Internet banking area. OCC
6. Gain an understanding of the bank's Internet banking business and disclosures by reviewing the bank's Web site. OCC
7. Prepare a general ledger balance comparison for all general ledger accounts related to Internet Banking. Obtain an explanation for all large differences.

Prior Audit and Examination Reports

1. Review the prior audit report and note items to be followed up during the current audit. Determine if management has taken appropriate and timely action to address the deficiencies noted in the audit report.
2. Review any examination reports received since the last audit. Determine if management has taken appropriate and timely action to address any deficiencies noted.

Internet Banking Products and Services

1. Obtain a description and/or diagram of the Internet banking system and its capabilities. Consider hardware, software, points of connectivity to internal systems, and remote access points. Evaluate:
 - How the Internet banking system is linked to other host systems or the network infrastructure in the bank.
 - How transactions and data flow through the network.
 - Potential areas of vulnerability. OCC
2. Obtain an overview of transaction and payment services flow and settlement processes and determine whether:
 - The bank's settlement responsibilities are clearly defined.

- The vendor's policies address uncollected funds, settlement, customer service, backup, contingency planning, and disaster recovery. OCC
3. Review the transaction and payment services products. Determine whether adequate control features are built into the systems to ensure authentication of the user, data integrity, and confidentiality of transactions. OCC
 4. Review any weblinking relationships with both affiliated and unaffiliated third parties.
 - Ascertain if sufficient due diligence was conducted on the third parties with which we formed weblinking relationships with respect to their ability to provide service and their overall information security and privacy policies.
 - Ensure formal contracts or agreements were negotiated that define the rights and responsibilities of the bank and third parties.
 - Determine if appropriate disclosures are displayed on the bank's website so that customers are not confused about which products and services are offered by the bank and which are offered by third parties in weblinking relationships. (OCC Bulletin 2001-31)

Implementation

1. Determine whether the board, or an appropriate committee, approved the Internet Banking system based on a written strategic plan and risk analysis. FDIC
2. Determine if management provides adequate training for all officers and staff affected by electronic banking systems, including those responsible for products, services, information systems, compliance, and legal issues. (Note: The training program should be ongoing). FDIC
3. Determine if management verifies the accuracy and content of financial planning software, calculators, and other interactive programs (between the bank and its customers) available through the systems. FDIC

Policies and Procedures

1. Determine whether the bank has established policies over hypertext links that enable consumers to clearly distinguish:
 - Insured and non-insured financial products.
 - Bank versus non-bank products.
 - When leaving the bank's Web site. OCC
2. Determine if policies and procedures governing access to and the disclosure of customers' confidential information are updated for electronic capabilities.
 - Determine if the policies address what information may be shared with third parties such as non-deposit product representatives, discount brokerage services, etc.
 - Determine if guidelines pertaining to confidential information are included as part of the contracts and agreements covering third party arrangements. FDIC
3. Review a sample of Internet Banking customers and ensure they are only allowed access to accounts for which they are authorized signers.
 - Commercial accounts may have users who are not authorized signers. However, they must be approved by an authorized signer on the account.
4. Determine how management monitors system performance (e.g., transaction volume, response times, availability / downtime, capacity reports, and customer service logs and complaint summaries.) FFIEC/FDIC The following provides various methods for reporting this information; determine those that would be appropriate for this organization and detail the method in which it is reviewed.
 - Number of visitors to the website

- "User Assets" information
- Number and volume of new Internet Banking loans for the month
- Number and volume of total Internet Banking loans as of the end of the month
- Volume of total loans outside our normal servicing area
- Volume of total deposits outside our normal servicing area
- All security threats or repeated unauthorized access attempts
- Any time during which the Internet Banking site was non-operational for four hours or longer.

Administration

1. Ascertain if an Internet Banking Security Officer has been named, as well as a backup.
2. On a sample basis, ascertain if users of the Internet Banking system have unique user IDs and passwords. Ensure passwords are changed quarterly
3. Ensure the ISP password and Master passwords are changed monthly
4. Determine if senior management establishes appropriate levels of access to information and applications for officers, employees, system vendors, customers, and other users. Determine if the access levels are enforced and reviewed on a regular basis (annually, per policy). FDIC
 - Review Employee Access to Internet Banking System forms.
5. Determine if management establishes adequate programs for customer service and support:
 - Review the organization and responsibilities of the customer support function.
 - If the customer support service is outsourced, note the responsibilities of the vendor and determine how management monitors customer problems, demands, or complaints.
 - Determine whether customer service levels have been established. If so, determine how management monitors adherence to service levels.
 - Determine how management assesses the adequacy of customer service.
 - Determine whether deficiencies exist in the process by reviewing problem logs or customer service reports and through discussions with management. FDIC/OCC
6. Determine if management generates and reviews exception reports on a periodic basis. FDIC
7. Tour the server location(s).
 - a) Determine if access to the console is controlled.
 - b) Determine if adequate fire detection and suppressant equipment is available.
 - c) Determine if the server is connected to an uninterruptible power supply (UPS) and whether it has been tested.
 - d) Determine that servers are protected from damage resulting from electric power surges and spikes.
 - e) Determine if housekeeping procedures are adequate to provide protection from food, liquids, dust, smoke, and magnetic fields.
8. Determine that the bank has an adequate electronic banking security program that addresses the following, as appropriate:
 - Access to, protection of, and disclosure of customers' confidential information
 - Methods for establishing the legitimacy of each party requesting an account action or submitting related instructions or data
 - What information may be shared with third-parties
 - The ability of third-party servicers to access or monitor electronic transmissions between the bank and any of its customers. FDIC

Accounting and Processing

1. Determine if the bank's periodic reconciliation procedures incorporate the full scope of transactional capabilities. Determine if the procedures apply to the general ledger and subsidiary accounts, as appropriate. FDIC
2. Ensure all general ledger accounts related to Internet Banking are reconciled on a timely basis.
 - a) Supervisory personnel should regularly review reconciliements and exception items.
 - b) Ascertain if reconciling items are adequately controlled.
 - c) Procedures for balancing should be well documented and monitored for adherence. FFIEC
3. Review all suspense accounts related to Internet Banking. Ensure all entries are valid. Trace large items to ascertain how they cleared.
4. Determine if procedures are in place to control customer transfers of uncollected funds from each access point. FDIC
5. Confirm that safeguards are in place to detect and prevent duplicate transactions within each system. FDIC
6. For systems that permit access to credit lines, determine if draws or credit extensions are adequately controlled. FDIC
7. Determine if appropriate audit trails are incorporated into each system. FDIC
8. Determine if the Daily Task Log is being completed daily and if a supervisor is reviewing it.
9. Ascertain if the following S1 reports are being reviewed daily by two employees for unusual or large items.
 - Summary Report
 - Manual To Do Report
 - FastPay Report
 - ACH Report
 - Federal ACH Report
 - Bill Payment Report
 - Notifications Report
10. Review customer comments, questions, and complaints logged since last audit. Ensure they were logged on the Customer Service Log and were handled timely.
11. On a sample basis, determine if the following were obtained for new deposit accounts opened through the Internet Banking system:
 - a) A credit check approved by an officer of the bank.
 - b) A review to determine if the account satisfied the bank's "Know-Your-Customer Policy."
 - c) If the account is foreign, a review of the Office of Foreign Assets Control list of specially designated persons.
 - d) Signed new account application or signature card.
 - e) A properly completed Internet Banking Account Services form (retail customers only).
12. On a sample basis, determine if the following were obtained for new certificate of deposit accounts opened through the Internet Banking system:
 - a) A signed new CD account application or CD signature card.
 - b) A review to determine if the account satisfied the bank's "Know-Your-Customer Policy."
 - c) If the account is foreign, a review of the Office of Foreign Assets Control list of specially designated entities.

- d) Evidence that CD disclosures were mailed or faxed to customers.
13. On a sample basis, determine if the following were obtained for new loan accounts opened through the Internet Banking system:
- Ensure no loan applications outside of the bank's normal trade area were approved to commercial customers.
 - A signed residential consumer loan application.
 - A signed note agreement.
 - Evidence that loan disclosures were mailed or faxed to customers.
14. Ascertain if annual financial statements have been received and reviewed for vendors that perform any major services related to Internet Banking. Policy . FFIEC
15. Obtain SAS 70 reports on all vendors that process ABTC customer information and perform the following steps:
- Ensure that management has identified all third parties related to Internet banking that process information for ABTC..
 - Review the findings in the SAS 70s and the management action plans. Ascertain if management has implemented the user controls that each SAS 70 recommends, if applicable.
 - Ascertain if management obtains a SAS 70 report from the vendors annually.
 - Ensure the period reviewed by the SAS 70s is six months or longer (up to a year).
16. Ensure agreements /contracts are in effect for all Internet Banking customers.
- The agreement should set forth the rights, responsibilities, and liability for each party. FFIEC/FDIC
 - Determine if the documents address the bank's authority to monitor, store, and retrieve electronic transmissions (including messages and data) between the bank and its customers. FDIC
17. Determine that written contingency and business resumption plans have been developed for failure of the Internet Banking system and/or communication lines. FFIEC
18. Determine whether the bank has an adequate process in place for Internet banking recovery including whether:
- Internet banking contingency and business resumption plans are reviewed and updated regularly.
 - Specific personnel and staff are responsible for initiating and managing Internet banking recovery plans.
 - The plan ensures that single points of failure for critical network points are adequately addressed.
 - The plan establishes strategies to recover hardware, software, communication links, and data files.
 - Adequate back up agreements and contracts are in place for external vendors or critical suppliers and if these backup arrangements are tested fully.
 - The response process assures that senior management and the board of directors are made aware of adverse events as dictated by the severity of damage and monetary loss.
 - Procedures are in place to bring security breaches to the attention of appropriate management and external entities (e.g., CERT, FBI, OCC, etc.) OCC
19. Ascertain if contingency and business resumption plans are tested on a regular basis. Ensure management:
- Requires annual testing of recovery processes and systems.
 - Addresses adverse test results in a timely manner.
 - Informs the board or executive management of test results. FFIEC/OCC
20. Review the backup policy. Determine the following:
- A policy exists that defines adequate backup frequency and retention periods for backup data.
 - The procedures relating to in-house and off-site storage of backup data and programs are adequate. Ensure critical backups are stored in a secure, off-site location. (Per policy, a backup will be made of the Internet Banking system configuration files and customer configuration files daily. These files will be taken off-site.) (FFIEC) A test of the Internet Banking system backup files is made on an annual basis.

21. Obtain a list of tapes, documentation, etc. that are to be stored off-site and verify their existence. FFIEC

Legal and Regulatory Matters

1. Review the website to ensure information regarding the following is accurate:
 - a) Security features
 - b) Customer service access and hours
 - c) Obtaining CRA information
 - d) Names of officers/employees
 - e) Branch locations and operating times FDIC
2. Determine if appropriate procedures exist to ensure compliance with Financial Record Keeping and Bank Secrecy Act requirements, including Know Your Customer guidelines. (Procedures should be established to identify potential money laundering activities.) FDIC/OCC
3. Review the website screens pertaining to deposit accounts for compliance with the following:
 - a) FDIC notice appropriately displayed. (Uninsured products or services clearly designated.) (12 CFR 328) OCC
 - c) Truth in Savings disclosures (Reg. DD)
 - d) Accuracy of APY and rates offered (Reg. DD)
 - e) Electronic Funds Transfer Act disclosures (Reg. E)
 - f) Expedited Funds Availability Act disclosures (Reg. CC)
 - g) Reg. D disclosures
4. Review the website screens pertaining to loans for compliance with the following:
 - a) Fair Housing Act signage
 - b) Truth in Lending disclosures (Reg. Z)
 - c) Accuracy of APR and rates offered (Reg. Z)
 - d) Equal Credit Opportunity disclosures regarding credit denials
 - e) Consumer Leasing Act regarding terms on offered leases (Reg. M)
5. Determine whether Office of Foreign Asset Control (OFAC) identification and reporting capabilities are maintained for Internet banking products and services. (OCC)
6. Determine whether management has established a warning banner for users, announcing that intruders are accessing a private computer and that unauthorized access or use is not permitted and constitutes a crime punishable by law (18 USC 1030). OCC
7. If the bank is aware of computer-related crimes, determine whether a suspicious activity report (SAR) was filed. (See AL 97-9.) OCC Note: Compliance with the Graham, Leach, Bliley Act (GLBA) was not reviewed, as it is examined in a separate audit.

Conclusion Procedures

1. Prepare Records of Audit Findings (RAFTs) listing weaknesses, deficiencies, violations, and other problems noted.
2. Discuss audit findings and recommendations with management.
3. Prepare audit report.

These steps are performed by Internal Audit in between Pricewaterhouse's examinations. Pricewaterhouse also reviews these areas. Note: The following sections were addressed by our external auditors during their examination: Policy, Vendor Management, Passwords, Firewalls, Physical Security, Encryption, Virus Detection and Prevention, Business Resumption and Contingency Planning, Digital Signatures and Certificate Authorities, Monitoring, Internet Service Providers, etc.

Primary Sources: Electronic Banking Safety and Soundness Examination Procedures, FDIC, June 1998 ("FDIC")
FFIEC IS Examination Handbook, 1996 ("FFIEC") Internet Banking, Comptroller's Handbook, October 1999
("OCC") Internet Banking Policy, National Bank of Commerce, September 2000 ("P") Last revised December 2001

The following steps were removed from the audit program because our external auditors covered these areas:

Administration

1. Assess the adequacy of the process for password administration for the Internet Banking System. Consider the following:
 - The adequacy of control and security over the bank's process for issuing passwords to customers.
 - Whether alphanumeric passwords are required.
 - The required length of passwords.
 - Whether passwords have an automatic expiration.
 - If adequate procedures are in place for resetting passwords.
 - If automatic log-off controls exist for user inactivity.
 - Whether excessive failed access attempts by the user disables access. OCC
2. Ascertain if access to the Internet Service Provider (ISP) password, Master Passwords, and S1 server password is appropriate.
3. Ensure that repeated failed attempts to gain access to information result in an automatic timeout.
4. Determine whether there is a direct / indirect connection between the bank's internal operating system(s) and the system that hosts the external electronic service or activity (for example, a web site). FDIC
5. Determine if procedures exist to monitor unauthorized attempts to access the bank's system.
 - Determine if the bank's policies require formal reporting in case of attempted or actual attacks against any of the bank's systems.
 - Review all known incidents and ensure they were reported to the proper authorities. FDIC
6. Determine whether the bank has an adequate process regarding virus detection and prevention associated with the Internet banking system. Consider whether:
 - User awareness efforts address viruses. OCC
 - The virus containment program is documented. FFIEC
 - Screening for viruses uses a virus detecting software package. FFIEC
 - The frequency with which anti-virus products and definitions are updated is adequate, and the most current version/release is installed. OCC
 - Virus detection software distribution is made through downloads from the bank's server. OCC/FFIEC
7. Determine whether the bank has an adequate process to address physical security for computer hardware, software, communication equipment, and communication lines associated with the Internet banking system including:
 - Whether the network servers are secured.
 - How the bank prevents unauthorized physical access to equipment.
 - Whether the bank secures vendor owned equipment.
 - If proper physical controls are in place for the data center housing equipment and documentation. FDIC/OCC
8. Determine if the bank entered formal contracts with each vendor. Determine if the contracts contain the following information and are reviewed by bank legal counsel, if appropriate:
 - Description of the work to be performed by the servicer.
 - Applications to be processed and services to be provided.
 - Responsibilities of both parties regarding addition or deletion of applications.

- Processing frequency and report generation.
 - Processing priorities for both normal and emergency situations. FFIEC/OCC
 - Rights, responsibilities, and liability for each party. FDIC
 - Basis of costs and description of additional fees.
 - Monthly processing fees, additional charges and free services, basis of fee calculations.
 - Ownership of any special software developed for bank. (Generally, the developer owns the product.)
 - Costs for satisfying special management requests, audit needs, and regulatory requirements.
 - Price changes. FFIEC/OCC
 - On-line communications availability, transmission line security, and transaction authentication. - Operating hours for on-line communication network.
 - Responsibilities for security of the communications network FFIEC/OCC
 - Audit rights and responsibilities. FFIEC/OCC
 - Contingency plans for service recovery, data backup, and record protection provisions.
 - Servicer's backup arrangements
 - Servicer's disaster recovery/contingency plan. FFIEC/OCC/FDIC
 - Access, ownership, and control of customer data and other confidential information. FFIEC/OCC/FDIC
 - Availability of financial information (preferably annually). FFIEC/OCC
 - Training. FFIEC/OCC
 - Reasonable penalty and cancellation provisions. FFIEC/OCC
 - Prohibition against assignment of contract by either party without the other's consent. FFIEC/OCC
 - Security precautions on the part of the service provider. FDIC
9. If the bank obtains software products from a vendor, ascertain if the vendor supplies source code or maintains a third-party escrow for the benefit of the serviced bank. If documentation and source code are held under Escrow Agreement, the agreement should include the following provisions:
- Conditions whereupon the bank can obtain the source programs and documentation.
 - The media in which the source programs will be released.
 - Arrangements for auditing the escrow arrangement. An assurance that the most current versions of source programs and documentation will be held by the escrow agent. (Obtain a third-party letter regarding this assurance on a regular basis.) FFIEC-12/OCC

Policies and Procedures

1. Determine whether Internet banking security policies include:
 - a) Clear lines of responsibility for system security - Review the duties of the security administrator. Determine if their authority is adequate to dictate controls and enforce policies.
 - b) Network and data access control. OCC
2. Determine whether Internet banking firewall policies address:
 - Responsibility for firewall maintenance and monitoring
 - Well-defined access rules
 - Access rules that dictate what traffic is allowed or forbidden. OCC
3. Determine whether encryption is adequately addressed in the security policy and the policy includes:
 - Who is responsible for control of encryption processes.
 - How encryption is used.
 - Data classification techniques.
 - Use of encryption to protect transmission of passwords, messages, or data during internal and open network communications sessions. OCC
4. Determine whether policies establish the use of virus detection software and note the products used. OCC

5. Identify whether security policies are periodically reviewed and updated and note whether the board of directors or senior management committee approves the policies. OCC