INFORMATION SYSTEMS AUDIT CHECKLIST

Internal and External Audit

(1) Internal audit program and/or policy
(2) Information relative to the qualifications and experience of the bank's internal auditor
(3) Copies of internal IS audit reports for the past two years
(4) Copies of most recent IS audits performed by regulatory agencies or other outside auditors
(5) All bank responses to IS audits or regulatory examinations
(6) Minutes of audit committee minutes

Management

(1) Organizational chart listing individuals responsible for IS along with job titles
(2) Any available biographical or certification data for key IS personnel
(3) Any available job descriptions
(4) Minutes of board of directors meetings for past twelve months
(5) Information about IS governance committees often called steering committees or technology committees as well as minutes of meetings for past twelve months
(6) Copies of all policies governing IS activity
(7) Copies of current IS insurance policies including coverage on: equipment and facilities, media reconstruction, items in transit, employee fraud, third-party fraud, business interruption, and errors and omissions
(8) Copies of information systems/information technology strategic plans

Vendor Management

(1) Schedule of all applications processed in-house including the name of software vendor and/or support vendor
(2) Schedule of all applications processed by a service bureau
(3) Any agreements with software, hardware, or network service providers used by the bank
(4) Service providers' audited financial statements and annual reports
(5) Any third-party reviews of service providers' controls over information technology and related processes such as SAS 70 reports
(6) Any information about the disaster recovery program and the testing of same for key service providers
(7) Any evidence documenting due diligence with respect to management of vendors such as the way primary outsourced vendor invoices are reviewed for accuracy
(8) Information about the bank's involvement in user groups
(9) Procedures for implementing core software vendor release updates

Development and Acquisition

(1) Procedures, policies or standards governing the acquisition of technology equipment or software systems and programs
(2) Information about any major development or acquisition projects (1) recently completed, (2) currently underway, or (3) planned for the future

(3) Information about any custom software which the bank has developed internally or which it has commissioned a company or person to develop
(4) Information about the development and use of query or data mining reports used by the bank
(5) Information about the management, organization, and storage of software licenses for software being utilized by the enterprise

Operations

(1) Schedule of all significant computer equipment including manufacturer, model, operating system if applicable, and as many other identifying characteristics as possible
(2) Operator check lists, user instructions, run books, or other documentation of this type
(3) Procedures designed to facilitate separation of operational duties
(4) Procedures relative to master file changes such as changes of address, due dates, etc.
(5) Procedures or policies relative to the handling of negotiable items
(6) Samples of any manual logs maintained to track IS-related events or problems

Information Security

(1) Any information relative to a formal information security program
(2) Any information relative to a formal risk assessment program
(3) Any external reports, studies, or assessments of risks relative to information security
(4) Diagrams or schematics of local and wide area networks
(5) Information about network access controls including firewalls, application access controls, remote access controls, etc.
(6) Information relative to the management, configuration, and monitoring of the network firewalls
(7) Lists and samples of any firewall-generated reports, logs or alerts
(8) Information relative to intrusion protection
(9) Authentication controls including password standards for the network as well as the host processor
(10) Lists and samples of any system-generated reports or logs or any special software used to automatically monitor and report system activity relative to either the network, or any ancillary systems
(11) Vulnerability assessments and/or penetration tests
(12) Information relative to security education of employees
(13) Nondisclosure agreements with vendors
(14) Any information about the use of virus protection software
(15) Information about physical security including locks, fire extinguishers, sprinklers, etc.
(16) Employee handbooks, standards, or policies
(17) Information about any disclosures or contracts signed by employees relative to information systems

Business Continuity

(1) Business continuity plan

(2) Emergency preparedness plans
(3) Inventory of offsite storage facilities
(4) Contracts with business continuity providers
(5) Schedule of equipment and other resources at the designated alternate processing site
(6) Reciprocal agreements with other banks or businesses
(7) Reports of recent business continuity tests
(8) Documentation of vendor assurances relative to business continuity
(9) Procedures, and/or schedules relative to the media backup of all data on all servers including standalone PCs, networked PCs, core processing system, and all ancillary systems

Fedline and Retail Payment Systems

(1) Business continuity plan
(2) Documentation relative to Fedline or Bankers Bank procedures
(2) Documentation relative to ATM administration
(3) Documentation relative to the issuance of ATM/debit cards
(4) Vendor contracts for ATM/ debit card services
(5) Procedures governing PIN administration
(6) Procedures relative to captured and returned cards
(7) Any information relative to ACH administration
(8) ACH policy
(9) ACH origination agreements with customers
(10) Recent NACHA or GACHA audits
(11) Any information relative to funds transfer administration

Electronic Banking

(1) Information regarding internet banking, telephone banking, and other electronic banking activities engaged in by the bank
(2) Procedures relative to customer user profiles and passwords
(3) Daily procedures carried out by employees relative to electronic banking
(4) Copies of policies and procedures governing electronic banking activities
(5) Copies of contracts with electronic banking vendors
(6) Network schematic to identify the location of major e-banking components
(7) Information relative to the number of customers who use the various electronic banking applications
(8) Information relative to risk assessment of electronic banking activities
(9) Information relative to the design and maintenance of the bank's website
(10) Information relative to the flow of information between the bank's electronic banking applications and the bank's core processing system