INFORMATION TECHNOLOGY SYSTEM REVIEW PROCEDURES

Management and Administration of IT Systems

- Review minutes of the Board of Directors and relevant committee meetings for evidence of Board and Senior Management support and supervision over the Bank's IT activities.
- Inquire into and review the adequacy of all IT policies (general usage, security, privacy, etc.) and procedure manuals.
- Determine if policies are established regulating staff Internet usage, downloading of software and electronic mail.
- Evaluate the Bank's restrictions on the use of computers and the data they contain and/or generate. This should include prohibitions against copying/piracy of software.
- Evaluate the adequacy of policies and procedures for authentication and access controls to manage effectively the risks to the Bank.

Internal IT Risk Assessment and Evaluation

- Review the membership list of board, IT steering, or relevant management committees established to review IT related matters. Determine if board, senior management, business lines, audit and IT personnel are represented appropriately and regular meetings are held.
- Review the minutes of the board of directors and relevant committee meetings for evidence of senior management support and supervision of IT activities.
- Determine if committees review, approve, and report to the board of directors on:
    - Information security risk assessment,
    - Short and long-term IT strategic plans,
    - IT operating standards and policies,
    - Resource allocation (e.g., major hardware/software acquisition and project priorities),
    - Status of major projects,
    - IT budgets and current operating cost,
    - Research and development studies, and
    - Corrective actions on significant audit and examination deficiencies.
- Determine if the board of directors or senior management gives adequate consideration to the following IT matters when formulating the institution's overall business strategy:
    - Risk assessment,
    - IT strategic plans,
    - Current status of the major projects in process or planned,
    - Staffing levels (sufficient to complete tasks as scheduled),
    - IT operating costs, and
    - IT contingency planning and business recovery.
- Review the strategic plans for IT activities. Determine if the goals and objectives are consistent with the institution's overall business strategy. Document significant changes made since the last examination or planned that affect the institution's organizational structure, hardware/software configuration, and overall data processing goals. Determine:
    - If business needs are realistic,
    - If IT has the ability to meet business needs,
    - If the strategic plan defines the IT environment,
    - If the plan lists strategic initiatives,

- If the plan explains trends and issues of potential impact, and
- If there are clearly defined goals and metrics.

- Review turnover rates in IT staff and discuss staffing and retention issues with:
  - IT management. Identify root causes of any staffing or expertise shortages including compensation plans or other retention practices.
- If IT employees have duties in other departments, determine if:
  - Management is aware of the potential conflicts such duties may cause, and
  - Conflicting duties are subject to appropriate supervision and compensating controls.
- Review the adequacy of insurance coverage (if applicable) for:
  - Employee fidelity,
  - IT equipment and facilities,
  - Media reconstruction,
  - E-banking,
  - EFT,
  - Loss resulting from business interruptions,
  - Errors and omissions,
  - Extra expenses, including backup site expenses,
  - Items in transit, and
  - Other probable risks (unique or specific risks for a particular institution). □□

Access Rights Controls and Authentication

Access Rights Administration

- Evaluate the adequacy of policies and procedures for authentication and access controls to manage effectively the risks to the financial institution.
  - Evaluate the processes that management uses to define access rights and privileges (e.g., software and/or hardware systems access) and determine if they are based upon business need requirements.
  - Review processes that assign rights and privileges and ensure that they take into account and provide for adequate segregation of duties.
  - Determine whether access rights are the minimum necessary for business purposes. If greater access rights are permitted, determine why the condition exists and identify any mitigating issues or compensating controls.
  - Ensure that access to operating systems is based on either a need-to-use or an event-by-event basis.
- Determine whether the user registration and enrollment process:
  - Uniquely identifies the user,
  - Verifies the need to use the system according to appropriate policy,
  - Enforces a unique user ID,
  - Assigns and records the proper security attributes (e.g., authorization),
  - Enforces the assignment or selection of an authenticator that agrees with the security policy,
  - Securely distributes any initial shared secret authenticator or token, and
  - Obtains acknowledgement from the user of acceptance of the terms of use.
- Determine whether employee's levels of online access (blocked, read-only, update, override, etc.)

match current job responsibilities.

- Determine that administrator or root privilege access is appropriately monitored, where appropriate.
    - Management may choose to further categorize types of administrator/root access based upon a risk assessment. Categorizing this type of access can be used to identify and monitor higher-risk administrator and root access requests that should be promptly reported.
- Evaluate the effectiveness and timeliness with which changes in access control privileges are implemented and the effectiveness of supporting policies and procedures.
    - Review procedures and controls in place and determine whether access control privileges are promptly eliminated when they are no longer needed. Include former employees and temporary access for remote access and contract workers in the review.
    - Assess the procedures and controls in place to change, when appropriate, access control privileges (e.g., changes in job responsibility and promotion).
    - Determine whether access rights expire after a predetermined period of inactivity.
    - Review and assess the effectiveness of a formal review process to periodically review the access rights to assure all access rights are proper. Determine whether necessary changes made as a result of that review.
- Determine that, where appropriate and feasible, programs do not run with greater access to other resources than necessary. Programs to consider include application programs, network administration programs (e.g., Domain Name System), and other programs.
- Compare the access control rules establishment and assignment processes to the access control policy for consistency.
- Determine whether users are aware of the authorized uses of the system.

Authentication

- Do internal users receive a copy of the authorized-use policy, appropriate training, and signify understanding and agreement before usage rights are granted?
- Is contractor usage appropriately detailed and controlled through the contract?
- Do customers and Web site visitors either explicitly agree to usage terms or are provided a disclosure, as appropriate?

- Determine whether the financial institution has removed or reset default profiles and passwords from new systems and equipment.
- Determine whether access to system administrator level is adequately controlled and monitored.
- Evaluate whether the authentication method selected and implemented is appropriately supported by a risk assessment.
- Evaluate the effectiveness of password and shared-secret administration for employees and customers considering the complexity of the processing environment and type of information accessed. Consider:
    - Confidentiality of passwords and shared secrets (whether only known to the employee/customer),
    - Maintenance of confidentiality through reset procedures,
    - The frequency of required changes (for applications, the user should make any changes from the initial password issued on enrollment without any other user's intervention),
    - Password composition in terms of length and type of characters (new or changed passwords should result in a password whose strength and reuse agrees with the security policy),
    - The strength of shared secret authentication mechanisms, and
    - Restrictions on duplicate shared secrets among users (no restrictions should exist).

- Determine whether all authenticators (e.g., passwords, shared secrets) are protected while in storage and during transmission to prevent disclosure.
    - Identify processes and areas where authentication information may be available in clear text and evaluate the effectiveness of compensating risk management controls.
    - Identify the encryption used and whether one-way hashes are employed to secure the clear text from anyone, authorized or unauthorized, who accesses the authenticator storage area.
- Determine whether passwords are stored on any machine that is directly or easily accessible from outside the institution, and if passwords are stored in programs on machines which query customer information databases. Evaluate the appropriateness of such storage and the associated protective mechanisms.
- Determine whether unauthorized attempts to access authentication mechanisms (e.g., password storage location) are appropriately investigated. Attacks on shared-secret mechanisms, for instance, could involve multiple log-in attempts using the same username and multiple passwords or multiple usernames and the same password.
- Determine whether authentication error feedback (i.e., reporting failure to successfully log-in) during the authentication process provides prospective attackers clues that may allow them to hone their attack. If so, obtain and evaluate a justification for such feedback.
- Determine whether adequate controls exist to protect against replay attacks and hijacking.
- Determine whether token-based authentication mechanisms adequately protect against token tampering, provide for the unique identification of the token holder, and employ an adequate number of authentication factors.
- Determine whether PKI-based authentication mechanisms:
    - Securely issue and update keys,
    - Securely unlock the secret key,
    - Provide for expiration of keys at an appropriate time period,
    - Ensure the certificate is valid before acceptance,
    - Update the list of revoked certificates at an appropriate frequency,
    - Employ appropriate measures to protect private and root keys, and
    - Appropriately log use of the root key.
- Determine that biometric systems:
    - Have an adequately strong and reliable enrollment process, adequately protect against the presentation of forged credentials (e.g., address replay attacks), and are appropriately tuned for false accepts/false rejects.
- Determine whether appropriate device and session authentication takes place, particularly for remote and wireless machines.
- Review authenticator reissuance and reset procedures. Determine whether controls adequately mitigate risks from:
    - Social engineering,
    - Errors in the identification of the user, and
    - Inability to re-issue on a large scale in the event of a mass compromise.

Network Security

- Evaluate the adequacy and accuracy of the network architecture.
    - Obtain a schematic overview of the financial institution's network architecture.
    - Review procedures for maintaining current information, including inventory reporting of how new hardware are added and old hardware is removed.

- Review audit and security reports that assess the accuracy of network architecture schematics and identify unreported systems.

- Evaluate controls that are in place to install new or change existing network infrastructure and to prevent unauthorized connections to the financial institution's network.
  - Review network architecture policies and procedures to establish new, or change existing, network connections and equipment.
  - Identify controls used to prevent unauthorized deployment of network connections and equipment.
  - Review the effectiveness and timeliness of controls used to prevent and report unauthorized network connections and equipment.
- Evaluate controls over the management of remote equipment.
- Determine whether effective procedures and practices are in place to secure network services, utilities, and diagnostic ports, consistent with the overall risk assessment.
- Determine whether external servers are appropriately isolated through placement in demilitarized zones (DMZs), with supporting servers on DMZs separate from external networks, public servers, and internal networks.
- Determine whether appropriate segregation exists between the responsibility for networks and the responsibility for computer operations.
- Determine whether network users are authenticated, and that the type and nature of the authentication (user and machine) is supported by the risk assessment. Access should only be provided where specific authorization occurs.
- Determine that, where appropriate, authenticated users and devices are limited in their ability to access system resources and to initiate transactions.
- Evaluate the appropriateness of technical controls mediating access between security domains. Consider:
  - Firewall topology and architecture,
  - Type(s) of firewall(s) being utilized,
  - Physical placement of firewall components,
  - Monitoring of firewall traffic,
  - Firewall updating,
  - Responsibility for monitoring and updating firewall policy, and
  - Placement and monitoring of network monitoring and protection devices, including intrusion detection system (IDS) and intrusion prevention system (IPS) functionality; and contingency planning.
- Determine whether firewall and routing controls are in place and updated as needs warrant.
  - Identify personnel responsible for defining and setting firewall rule sets and routing controls.
  - Review procedures for updating and changing rule sets and routing controls.
  - Confirm that the ruleset is based on the premise that all traffic that is not expressly allowed is denied, and that the firewall's capabilities for identifying and blocking traffic are effectively utilized.
  - Confirm that network mapping through the firewall is disabled.
  - Confirm that network address translation (NAT) and split DNS are used to hide internal names and addresses from external users.
  - Confirm that malicious code is effectively filtered.
  - Confirm that firewalls are backed up to external media, and not to servers on protected networks.

- Determine that firewalls and routers are subject to appropriate and functioning host controls.
- Determine that firewalls and routers are securely administered.
- Confirm that routing tables are regularly reviewed for appropriateness on a schedule commensurate with risk.

- Determine whether network-based IDSs are properly coordinated with firewalls (see "Security Monitoring" procedures).
- Determine whether logs of security-related events and log analysis activities are sufficient to affix accountability for network activities, as well as support intrusion forensics and IDS. Additionally, determine that adequate clock synchronization takes place.
- Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.
- Determine whether appropriate filtering occurs for spoofed addresses, both within the network and at external connections, covering network ingress and egress.
- Determine whether appropriate controls exist over the confidentiality and integrity of data transmitted over the network (e.g., encryption, parity checks, message authentication).
- Determine whether appropriate notification is made of requirements for authorized use, through banners or other means.
- Determine whether remote access devices and network access points for remote equipment are appropriately controlled.
  - Remote access is disabled by default, and enabled only by management authorization.
  - Management authorization is required for each user who accesses sensitive components or data remotely.
  - Authentication is of appropriate strength (e.g., two-factor for sensitive components).
  - Modems are authorized, configured, and managed to appropriately mitigate risks.
  - Appropriate logging and monitoring takes place.
  - Remote access devices are appropriately secured and controlled by the institution.
- Determine whether an appropriate archive of boot disks, distribution media, and security patches exists.
- Evaluate the appropriateness of techniques that detect and prevent the spread of malicious code across the network.

Host Security

- Determine whether hosts are hardened through the removal of unnecessary soft- ware and services, consistent with the needs identified in the risk assessment, that configuration takes advantage of available object, device, and file access controls, and that necessary software updates are applied.
- Determine whether the configuration minimizes the functionality of programs, scripts, and plug-ins to what is necessary and justifiable.
- Determine whether adequate processes exist to apply host security updates, such as patches and anti-virus signatures, and that such updating takes place.
- Determine whether new hosts are prepared according to documented procedures for secure configuration or replication, and that vulnerability testing takes place prior to deployment.
- Determine whether remotely configurable hosts are configured for secure remote administration.
- Determine whether an appropriate process exists to authorize access to host systems and that authentication and authorization controls on the host appropriately limit access to and control the access of authorized individuals.

- Determine whether access to utilities on the host are appropriately restricted and monitored.
- Determine whether the host-based IDSs identified as necessary in the risk assessment are properly installed and configured, that alerts go to appropriate individuals using an out-of-band communications mechanism, and that alerts are followed up. (Coordinate with the procedures listed in "Security Monitoring.")
- Determine whether logs are sufficient to affix accountability for host activities and to support intrusion forensics and IDS and are appropriately secured for a sufficient time period.
- Determine whether vulnerability testing takes place after each configuration change.
- Determine whether appropriate notification is made of authorized use, through banners or other means.
- Determine whether authoritative copies of host configuration and public server content are maintained off line.
- Determine whether an appropriate archive of boot disks, distribution media, and security patches exists.
- Determine whether adequate policies and procedure govern the destruction of sensitive data on machines that are taken out of service.

User Equipment Security (E.G., workstation, laptop, handheld)

- Determine whether new user equipment is prepared according to documented procedures for secure configuration or replication and that vulnerability testing takes place prior to deployment.
- Determine whether user equipment is configured either for secure remote administration or for no remote administration.
- Determine whether adequate inspection for, and removal of, unauthorized hardware and software takes place.
- Determine whether adequate policies and procedures exist to address the loss of equipment, including laptops and other mobile devices. Such plans should encompass the potential loss of customer data and authentication devices.
- Determine whether adequate policies and procedures govern the destruction of sensitive data on machines that are taken out of service and that those policies and procedures are consistently followed by appropriately trained personnel.
- Determine whether appropriate user equipment is deactivated after a period of inactivity through screen saver passwords, server time-outs, powering down or other means.
- Determine whether systems are appropriately protected against malicious software such as Trojan horses, viruses, and worms.

Physical Security

- Determine whether physical security for information technology assets is coordinated with other security functions.
- Determine whether sensitive data in both electronic and paper form is adequately controlled physically through creation, processing, storage, maintenance, and disposal.
- Determine whether:
    - Authorization for physical access to critical or sensitive information-processing facilities is granted according to an appropriate process,
    - Authorizations are enforceable by appropriate preventive, detective, and corrective controls, and
    - Authorizations can be revoked in a practical and timely manner.
- Determine whether information processing and communications devices and transmissions are appropriately protected against physical attacks perpetrated by individuals or groups, as well as against environmental damage and improper maintenance. Consider the use of halon gas, computer encasing,

smoke alarms, raised flooring, heat sensors, notification sensors, and other protective and detective devices.

Personnel Security

- Determine whether the institution performs appropriate background checks on its personnel during the hiring process and thereafter, according to the employee's authority over the institution's systems and information.
- Determine whether the institution includes in its terms and conditions of employment the employee's responsibilities for information security.
- Determine whether the institution requires personnel with authority to access customer information and confidential institution information to sign and abide by confidentiality agreements.
- Determine whether the institution provides to its employees appropriate security.
- Training covering the institution's policies and procedures, on an appropriate frequency and those institution employees certify periodically as to their understanding and awareness of the policy and procedures.
- Determine whether employees have an available and reliable mechanism to promptly report security incidents, weaknesses, and software malfunctions.
- Determine whether an appropriate disciplinary process for security violations exists and is functioning.

Application Security

- Determine whether software storage, including program source, object libraries, and load modules, are appropriately secured against unauthorized access.
- Determine whether user input is validated appropriately (e.g., character set, length, etc).
- Determine whether appropriate message authentication takes place.
- Determine whether access to sensitive information and processes require appropriate authentication and verification of authorized use before access is granted.
- Determine whether re-establishment of any session after interruption requires normal user identification, authentication, and authorization.
- Determine whether appropriate warning banners are displayed when applications are accessed.
- Determine whether appropriate logs are maintained and available to support incident detection and response efforts.

Software Development and Acquisition

- Inquire about how security control requirements are determined for software, whether internally developed or acquired from a vendor.
- Determine whether management explicitly follows a recognized security standard development process, or adheres to widely recognized industry standards.
- Determine whether the group or individual establishing security control requirements has appropriate credentials, background, and/or training.
- Evaluate whether the software acquired incorporates appropriate security controls, audit trails, and activity logs and that appropriate and timely audit trail and log reviews and alerts can take place.
- Evaluate whether the software contains appropriate authentication and encryption.
- Evaluate the adequacy of the change control process.
- Evaluate the appropriateness of software libraries and their access controls.
- Inquire about the method used to test the newly developed or acquired software for vulnerabilities.
    - For manual source code reviews, inquire about standards used, the capabilities of the reviewers, and the results of the reviews.

- If source code reviews are not performed, inquire about alternate actions taken to test the software for covert channels, backdoors, and other security issues.
- Whether or not source code reviews are performed, evaluate the institution's assertions regarding the trustworthiness of the application and the appropriateness of the network and host level controls mitigating application risk.

- Evaluate the process used to ascertain software trustworthiness. Include in the evaluation management's consideration of the:
  - Development process
    - Establishment of security requirements
    - Establishment of acceptance criterion
    - Use of secure coding standards
    - Compliance with security requirements
    - Background checks on employees
    - Code development and testing processes
    - Signed non-disclosure agreements
    - Restrictions on developer access to production source code
    - Physical security over developer work areas
  - Source code review
    - Automated reviews
    - Manual reviews
  - Vendor or developer history and reputation
    - Vulnerability history
    - Timeliness, thoroughness, and candidness of the response to security issues
    - Quality and functionality of security patches
- Evaluate the appropriateness of management's response to assessments of software trustworthiness:
  - Host and network control evaluation
  - Additional host and network controls

Service Provider Oversight-Security

- Determine whether contracts contain security requirements that at least meet the objectives of the 501(b) guidelines and contain nondisclosure language regarding specific requirements.
- Determine whether the institution has assessed the service provider's ability to meet contractual security requirements.
- Determine whether appropriate controls exist over the substitution of personnel on the institution's projects and services.
- Determine whether appropriate security testing is required and performed on any code, system, or service delivered under the contract.
- Determine whether appropriate reporting of security incidents is required under the contract.
- Determine whether institution oversight of third-party provider security controls is adequate.
- Determine whether any third party provider access to the institution's system is controlled according to "Authentication and Access Controls" and "Network Security" procedures.
- Determine whether the contract requires secure remote communications, as appropriate.
- Determine whether the institution appropriately assessed the third party provider's procedures for hiring and monitoring personnel who have access to the institution's systems and data.
- Determine whether the third party service provider participates in an appropriate industry ISAC.

Encryption

- Review the information security risk assessment and identify those items and areas classified as requiring encryption.
- Evaluate the appropriateness of the criteria used to select the type of encryption/cryptographic algorithms.
    - Consider if cryptographic algorithms are both publicly known and widely accepted (e.g., RSA, SHA, Triple DES, Blowfish, Twofish, etc.) or banking industry standard algorithms.
    - Note the basis for choosing key sizes (e.g., 40-bit, 128-bit) and key space.
    - Identify management's understanding of cryptography and expectations of how it will be used to protect data.
- Determine whether cryptographic key controls are adequate.
    - Identify where cryptographic keys are stored.
    - Review security where keys are stored and when they are used (e.g., in a hardware module).
    - Review cryptographic key distribution mechanisms to secure the keys against unauthorized disclosure, theft, and diversion.
    - Verify that two persons are required for a cryptographic key to be used, when appropriate.
    - Review audit and security reports that review the adequacy of cryptographic key controls.
- Determine whether adequate provision is made for different cryptographic keys for different uses and data.
- Determine whether cryptographic keys expire and are replaced at appropriate time intervals.
- Determine whether appropriate provisions are made for the recovery of data should a key be unusable.
- Determine whether cryptographic keys are destroyed in a secure manner when they are no longer required.

Data Security

- Obtain an understanding of the data security strategy.
    - Identify the financial institution's approach to protecting data (e.g., protect all data similarly, protect data based upon risk of loss).
    - Obtain and review the risk assessment covering financial institution data. Determine whether the risk assessment classifies data sensitivity in a reasonable manner and consistent with the financial institution's strategic and business objectives.
    - Consider whether policies and procedures address the protections for data that is sent outside the institution.
    - Identify processes to periodically review data sensitivity and update corresponding risk assessments.
- Verify that data is protected consistent with the financial institution's risk assessment.
    - Identify controls used to protect data and determine if the data is protected throughout its life cycle (i.e., creation, storage, maintenance, transmission, and disposal) in a manner consistent with the risk assessment.
    - Consider data security controls in effect at key stages such as data creation/acquisition, storage, transmission, maintenance, and destruction.
    - Review audit and security review reports that summarize if data is protected consistent with the risk assessment.
- Determine whether individual and group access to data is based on business needs.
- Determine whether, where appropriate, the system securely links the receipt of information with the originator of the information and other identifying information, such as date, time, address, and other

relevant factors.

Security Monitoring

- Identify the monitoring performed to identify non-compliance with institution security policies and potential intrusions.
    - Review the schematic of the information technology systems for common security monitoring devices.
    - Review security procedures for report monitoring to identify unauthorized or unusual activities.
    - Review management's self-assessment and independent testing activities and plans.
- Determine whether users are appropriately notified regarding security monitoring.
- Determine whether the activity monitoring sensors identified as necessary in the risk assessment process are properly installed and configured at appropriate locations.
- Determine whether an appropriate firewall ruleset and routing controls are in place and updated as needs warrant.
    - Identify personnel responsible for defining and setting firewall rulesets and routing controls.
    - Review procedures for updating and changing rulesets and routing controls.
    - Determine that appropriate filtering occurs for spoofed addresses, both within the network and at external connections, covering network entry and exit.
- Determine whether logs of security-related events are sufficient to support security incident detection and response activities, and that logs of application, host, and network activity can be readily correlated.
- Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.
- Determine whether logs are appropriately centralized and normalized, and that controls are in place and functioning to prevent time gaps in logging.
- Determine whether an appropriate process exists to authorize employee access to security monitoring and event management systems and that authentication and authorization controls appropriately limit access to and control the access of authorized individuals.
- Determine whether appropriate detection capabilities exist related to:
    - Network related anomalies, including;
        - Blocked outbound traffic
        - Unusual communications, including communicating hosts, times of day, protocols, and other header-related anomalies
        - Unusual or malicious packet payloads
    - Host-related anomalies, including;
        - System resource usage and anomalies
        - User related anomalies
        - Operating and tool configuration anomalies
        - File and data integrity problems
        - Anti-virus, anti-spyware, and other malware identification alerts
        - Unauthorized access
        - Privileged access
- Evaluate the institution's self-assessment plan and activities, including:
    - Policies and procedures conformance,

    - Service provider oversight,
    - Vulnerability scanning,
    - Configuration verification,
    - Information storage,
    - Risk assessment and monitoring plan review, and
    - Test reviews.
- Evaluate the use of metrics to measure:
    - Security policy implementation,
    - Security service delivery effectiveness and efficiency, and
    - Security event impact on business processes,
- Evaluate independent tests, including penetration tests, audits, and assessments. Consider:
    - Personnel,
    - Scope,
    - Controls over data integrity, confidentiality, and availability,
    - Confidentiality of test plans and data, and
    - Frequency.
- Determine that the functions of a security response center are appropriately governed by implemented policies addressing:
    - Monitoring,
    - Classification,
    - Escalation,
    - Reporting, and
    - Intrusion declaration.
- Determine whether an intrusion response team:
    - Contains appropriate membership,
    - Is available at all times,
    - Has appropriate training to investigate and report findings,
    - Has access to back-up data and systems, an inventory of all approved hardware and software, and monitored access to systems (as appropriate),
    - Has appropriate authority and timely access to decision makers for actions that require higher approvals, and
    - Have procedures for submitting appropriate incidents to the industry ISAC.
- Evaluate the appropriateness of the security policy in addressing the review of compromised systems. Consider
    - Documentation of the roles, responsibilities and authority of employees and contractors, and
    - Conditions for the examination and analysis of data, systems, and networks.
- Determine whether the information disclosure policy indicates what information is shared with others, in what circumstances, and identifies the individual(s) who have the authority to initiate disclosure beyond the stated policy.
- Determine whether the information disclosure policy addresses the appropriate regulatory reporting requirements.
- Determine whether the security policy provides for a provable chain of custody for the preservation of potential evidence through such mechanisms as a detailed action and decision log indicating who made each entry.

- Determine whether the policy requires all compromised systems to be restored before reactivation, through either rebuilding with verified good media or verification of software cryptographic checksums.
- Determine whether all participants in security monitoring and intrusion response are trained adequately in the detection and response policies, their roles, and the procedures they should take to implement the policies.
- Determine whether response policies and training appropriately address unauthorized disclosures of customer information, including:
    - Identifying the customer information and customers effected,
    - Protecting those customers through monitoring, closing, or freezing accounts,
    - Notifying customers when warranted, and
    - Appropriately notifying its primary federal regulator.
- Determine whether an effective process exists to respond in an appropriate and timely manner to newly discovered vulnerabilities. Consider:
    - Assignment of responsibility,
        - Prioritization of work to be performed
        - Appropriate funding
    - Monitoring, and
    - Follow-up activities.

E-Banking

- Determined whether the institution's written security program for customer information required by GLBA guidelines includes e-banking products and services.
- Determined whether the security program includes monitoring of systems and transactions and whether exceptions are analyzed to identify and correct noncompliance with security policies as appropriate.
- Determined the adequacy of the institution's authentication methods and need for multi-factor authentication relative to the sensitivity of systems or transactions.
- Determined if the institution uses passwords for customer authentication, determine whether password administration guidelines adequately address the following:
    - Selection of password length and composition considering ease of remembering, vulnerability to compromise, sensitivity of system or information protected, and use as single- or multi-factor authentication,
    - Restrictions on the use of automatic log-on features,
    - User lockout after a number of failed log-on attempts – industry practice is generally no more than 3 to 5 incorrect attempts,
    - Password expiration for sensitive internal or high-value systems,
    - Users' ability to select and/or change their passwords,
    - Passwords disabled after a prolonged period of inactivity,
    - Secure process for password generation and distribution,
    - Termination of customer connections after a specified interval of inactivity – industry practice is generally not more than 10 to 20 minutes,
    - Procedures for resetting passwords, including forced change at next log-on after reset,
    - Review of password exception reports,
    - Secure access controls over password databases, including encryption of stored passwords,
    - Password guidance to customers and employees regarding prudent password selection and the importance of protecting password confidentiality, and

    - Avoidance of commonly available information (i.e., name, social security number) as user IDs.
- Evaluated access control associated with employee's administrative access to ensure:
    - Administrative access is assigned only to unique, employee-specific IDs,
    - Account creation, deletion, and maintenance activity is monitored, and
    - Access to funds-transfer capabilities is under dual control and consistent with controls over payment transmission channel (e.g., ACH, wire transfer, FedLine).
- Evaluated the appropriateness of incident response plans.
- Assessed whether the information security program includes independent security testing as appropriate for the type and complexity of e-banking activity. Tests should include, as warranted:
    - Independent audits,
    - Vulnerability assessments, and
    - Penetration testing.
- Determined whether employee authorization levels and access privileges are commensurate with their assigned duties and reinforce segregation of duties.
- Determined whether controls for e-banking applications include:
    - Appropriate balancing and reconciling controls for e-banking activity,
    - Protection of critical data or information from tampering during transmission and from viewing by unauthorized parties (e.g., encryption),
    - Automated validation techniques such as check digits or hash totals to detect tampering with message content during transmission,
    - Independent control totals for transactions exchanged between e-banking applications and legacy systems, and
    - Ongoing review for suspicious transactions such as large-dollar transactions, high transaction volume, or unusual account activity.
- Determined whether audit trails for e-banking activities are sufficient to identify the source of transactions.
- Evaluated the physical security over e-banking equipment, media, and communication lines.
- Determined whether business continuity plans appropriately address the business impact of e-banking products and services.
- Assessed the adequacy of ongoing vendor oversight.
- Determined whether the institution has reviewed vendor contracts to ensure that the responsibilities of each party are appropriately identified.
- Assessed the adequacy of management's due diligence activities prior to vendor selection.
- Determined whether audit coverage of e-banking activities is appropriate for the type of services offered and the level of risk assumed. Consider the frequency of e-banking reviews, the adequacy of audit expertise relative to the complexity of e-banking activities, the extent of functions outsourced to third-party providers.

FedLine Access

- Identify the FedLine Advantage transmission method (Private Dial, internet or Frame Realy Customer Premise Equipment (CPE) and configuration (network-connected or standalone).
- Ensure that the VPN or Frame Relay CPE is in a secure location, subject to tight physical security, with access limited to authorized personnel.
- Determine how tokens are being safeguarded and the number of tokens available at the Bank.
- Verify whether FedLine computer/s are designated and have been configured for access to FedLine Advantage.

- Determine that the FedLine passwords and pass-phrases are secured and not written down near any FedLine designated machines.
- Determine whether the FedLine computer/s has a power-on password option. If there is no power on password option, evaluate the Bank's ability to control staff members assigned the Local Administrative access level, access to the FedLine computer/s.
- Verify that PCs are placed so that monitors and keyboards cannot be easily observed.
- Verify that anti-virus software is installed and configured to be active at all times on the PCs authorized to access FedLine Advantage.
- Determine whether personal firewall software is installed and is active on each Subscriber PC used in connection with FedLine Advantage, personal firewall software can not be disabled by the Subscriber, personal firewall is appropriately configured to allow only necessary ports and services.
- Verify that PCs authorized to access FedLine Advantage are included in the organization's overall network security structure and are sufficiently protected.
- Determine if the financial institution observe proper segregation of duties.
- Ensure that the changes to the VPN device and supporting network components are made using an established change control and approval process.
- Verify that the Bank has incorporated FedLine Advantage into their corporate information security program.
- Verify that only authorized PCs have FedLine Advantage Connection Utility and FedLine Security Token Driver software installed and have access to the VOP device. Additionally, obtain a list of all VPN devices and/or Frame Relay CPEs.
- Verify that FedLine Advantage documentation and the installation software CDs (FedLine Advantage Connection Utility and FedLine Security Token driver software) are treated as confidential.
- Confirm that the latest security patches are installed and functioning appropriately.

Social Engineering

- Evaluate policies and procedures for social engineering.
- Determine a target and:
    - Evaluate obtainable information
    - Determine if there is any information specific to the organization that should be given special consideration.
    - Evaluate risks associated with the target.
- Identify who could provide access to the targets (employees, other vendors, employee family members)?
- Evaluate for each target, the created profile including accessory information (work schedules of entry points, other passwords, knowledge of physical security, phone numbers, etc.).
- Determine attack methods using target profiles using attack scripts:
- Determine attack avenues which may include:
    - Phone calls
    - Email
    - Personal conversations.

Automated Clearing House (ACH)

- Determine if telecommunications lines used to receive data from customers and to transmit data to ACH operators are encrypted.
- Determine if a written contingency plan exists for ACH processing.

- Determine if ACH activities are considered in the Bank's overall business continuity plan and insurance program.

External Penetration Test

- Identify the external footprint vulnerabilities for appropriate security and access controls which include:
  - Online telephone directory searches.
  - Web site(s) reviewed for information gatherings.
  - Internet domain name registration searches.
  - American Registry of internet Number (ARIN) searches.
  - Domain name service (DNS) lookups.
  - Trace routes of public systems.
- Evaluate external intrusion systems for effectiveness to include:
  - Router testing.
  - Firewall testing.
  - Web server testing.
  - Electronic mail server testing.
  - Ping scans of public IP address blocks.
  - Port scans of public systems.
  - Ethical intrusion testing using commercial and public domain tools.

Business Disaster Recovery

- Evaluate the written Business Continuity Plan (BCP).
- Determine if the Bank has addressed pandemic risk in its BCP along with a preventive program, a documented strategy scaled to the stages of a pandemic outbreak, a comprehensive framework to ensure the continuance of critical operations, a testing program and an oversight program to ensure that the plan is reviewed and updated as required by interagency guidelines.
- Determine the following:
  - Bank has procedures in place to ensure the BCP is updated periodically but no less than annually.
  - Bank critical resources and technologies were covered by the BCP.
  - Information for the entire network and communication connections were included in the plan.
  - The plan establishes processing priorities to be followed in the event not all applications can be processed.
  - The board has established an enterprise-wide business continuity planning process appropriate for the size and complexity of the organization.
  - Management has been assigned responsibility to oversee the development, implementation, testing, and maintenance of the BCP.
  - Adequate resources, including sufficient human resources, are devoted to the business continuity process.
  - Board review and approval of the written BCP and testing results at least annually and documentation of the reviews in the board minutes.
  - Senior management review and prioritization of each business process and department for its critical importance and recovery prioritization on a periodic basis.
  - Senior management has evaluated the adequacy of the BCP for its critical service providers.
  - If satisfactory consideration has been given to geographic diversity for alternate location.
  - All functions and departments were included in the Business Impact Analysis (BIA).
  - Consideration of reputation, operational, compliance and other risks were considered in the plan.

- Review the BIA to determine if the identification and prioritization of business functions are adequate.
- Determine if the BIA identified maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, and the cost and recovery time objectives associated with downtime.
- Review the risk assessment to determine that it includes scenarios and probability of occurrence of disruptions of information services, technology, personnel, facilities, and service providers from internal and external sources.
- Determine if the risk assessment and BIA have been reviewed and approved by senior management and the board.
- Ensure policies address business continuity planning issues such as employee training, communication planning, insurance, government and community coordination.
- Determine if the Bank has conducted testing of the alternate location and if systems undergo similar testing as the primary location and systems.
- Determine whether appropriate access controls and physical controls have been considered and planned for the replicated production system and networks when processing is transferred to a substitute facility.
- Determine if the intrusion detection and response plan considers the resource availability, facility and systems changes that may exist when alternate locations are placed in use.
- Evaluate the procedure for granting temporary access to personnel during the implementation of contingency plans.
    - Evaluate the extent to which back-up personnel have been assigned different tasks when contingency planning scenarios are in effect and the need for different levels of systems, operational, data and facilities access.
    - Review the assignment of authentication and authorization credentials to see if they are based upon primary job responsibilities or if they also include contingency planning responsibilities.
- Review system documentation and evaluated for use in regular maintenance and disaster recovery situations.
- Determine that procedures have been developed and enforced for periodic backup of critical information.
- Determine that procedures are in place for periodic testing of restore capabilities.
- Determine that the disaster recovery and business resumption plans have been tested. Requested last test date and results.
- Determine that there are plans in place that address the return to normal operations and original business locations once the situation has been resolved and permanent facilities are again available.
- Determine that adequate documentation is housed at the alternate recovery location including copies of each BCP and copies of necessary system documentation.
- Determine if the Bank has a copy of the TSP's BCP(s) and incorporates it, as appropriate, into their plans.
- Determine if management has received and reviewed testing results of their TSPs.
- Determine if Bank management has assessed the adequacy of the TSP's business continuity program through their vendor management program (e.g. contract requirements, SAS 70 reviews).
- Through inquiries determine that adequate physical security and access controls exist over data back-ups throughout their life cycle, including when they are created, transmitted/taken to storage, stored, retrieved and loaded, and destroyed.
    - Review the risk assessment to identify key control points in a data set's life cycle.
    - Verify controls are in place consistent with the level of risk presented.
- Determine whether adequate physical security and access controls exist over data back-ups and program libraries throughout their life cycle, including when they are created, transmitted/taken to

storage, stored, retrieved and loaded, and destroyed.

- Review the risk assessment to identify key control points in a data set's life cycle.
- Verify controls are in place consistent with the level of risk presented.

Identity Theft "Red Flags" and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

- Determine if the Bank has performed a risk assessment that identifies whether the Bank offers or maintains covered accounts as described in section .90(b)(3)(ii) of the Act (accounts other than consumer accounts), taking into consideration the following:
  - The methods it provides to open its accounts.
  - The methods it provides to access its accounts
  - Its previous experiences with identity theft.
- Determine if the policies and procedures cover the following four basic elements required by the Regulation:
  - Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Bank's program.
  - Detect Red Flags that have been incorporated into the Program.
  - Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
  - Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.
- Determine if the policies and procedures have been approved by the board of directors or an assigned committee.
- Determine if procedures provide for proper board oversight related to development, implementation and administration of the Program, training staff, and overseeing service provider arrangements.
- Determine if the Bank has established reasonable internal controls to protect account holders sensitive personal information as part of their Information Security policies and procedures.
- Determine if the Bank has established reasonable policies and procedures if sensitive personal information is compromised as part of the Bank's Incident Response policies and procedures.
- Determine if the Bank has established due diligence procedures for vendors with access to sensitive data and that as part of the contract the Bank requires applicable service providers to have policies and procedures that will detect identity theft red flags that may arise in the performance of the service provider's activities as part of its Vendor Management policies and procedures.