USAID
FROM THE AMERICAN PEOPLE

MANUAL FOR THE ON AND OFF-SITE SUPERVISION OF CREDIT REFERENCE BUREAUS

CENTRAL BANK OF KENYA

SEPTEMBER 2010

This publication was produced for review by the United States Agency for International Development. It was prepared by Guillermo Bolanos for DAI and the Central Bank of Kenya.

MANUAL FOR THE ON AND OFF-SITE SUPERVISION OF CREDIT REFERENCE BUREAUS

CENTRAL BANK OF KENYA

Program Title:	Kenya Access to Rural Finance Program
Sponsoring USAID Office:	USAID/Kenya
Contract Number:	GEG-I-00-02-00011-00/215
Contractor:	DAI
Date of Publication:	September 2010

The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

TABLE OF CONTENTS

This page is intentionally blank

PREFACE

This Manual provides guidance to Central Bank of Kenya supervisors for the direct supervision of credit reference bureaus, and the indirect supervision of the national credit reference system, and for the different parties, not only the licensed credit reference bureaus and the regulated financial institutions, but also other data providers and subscribers and the subjects of credit reports.

The Manual proposes that supervisors consider:

1. The respective duties of the various participants in the credit information system, including credit seekers, and the effects on bona fide participants –data providers, credit reference bureaus, and subscribers- who follow the Central Bank of Kenya Regulations and Rules;

2. The coverage of credit information to more than credit-related financial transaction contracts, to include: credit related *applications*; *non financial* credit related transactions, and key persons involved – co-applicants, co-signers, and guarantors;

3. The comprehensive and non selective provision of client credit histories by data providers;

4. Central Bank monitoring the methodology used by credit reference bureaus, and of the use by subscribers, of credit scoring and other services to assess the credit worthiness of applicant classes;

5. Other activities and services of credit reference bureaus, to include:

   a. credit worthiness assessments;
   b. verification / processing of credit application information;
   c. cross-default notices or “watch services”;
   d. data storage and statistical research;
   e. tracing services of debtors and guarantors;
   f. verification of employment, income, address, and assets;
   g. collateral registry services; and,
   h. services for the prevention and detection of fraud

BACKGROUND

ON CREDIT BUREAUS

Creditors have a disadvantage versus the loan applicant to know all pertinent information on a credit application, known as moral hazard.

Credit Bureaus are information brokers. They may be set up by lenders and operated by them, or they may be for-profit institutions that provide detailed data.

Information sharing among lenders attenuates adverse selection and moral hazard and can therefore increase lending and reduce moral hazard. There are economies of scale, and the larger the data base of a credit bureau, the more complete and accurate its information. In addition:

- Credit bureaus enable lenders to lend to more and better risk clients (avoiding habitual defaulters) and to better determine (and lower) the interest rate spread that they need to cover expected losses of extending credit to good payers;
- Credit bureaus reduce moral hazard by developing a credit culture where they operate, as borrowers become aware that the credit market becomes aware of their credit history, and rewards or punishes them accordingly;
- Credit bureaus reduce the borrowing cost to the public as creditors compete for good borrowers. Those lower costs for good credit risks motivate borrowers to be more careful with repayment.

Thus, in competitive markets, "information sharing improves the pool of borrowers, decreases defaults and reduces interest rates."

Credit bureaus provide creditors with reliable, relevant and comprehensive data on the repayment habits and current debt of their credit applicants. Under reciprocity agreements, credit bureaus obtain data from creditors and other sources, consolidate and package information into individual reports, and distribute it to creditors for a fee.

The population covered by credit bureaus is mostly the middle to lower income segments of the population. In developing countries, this means the middle, lower middle and working classes, excluding the subsistence and upper classes.

A modern credit bureau acts as the specialized information channel and is the efficient and effective way to quickly gather, file, organize and provide credit reports in a massive scale.

Data accuracy is a goal shared by all participants. The avoidance, reduction, or correction of data inaccuracies or mistakes should be designed carefully to promote a fluid and cost-effective information exchange system. This is particularly crucial as a clean credit record increasingly becomes a necessity for access by individuals and firms to financing and other services.

The role of the supervisor is to ensure compliance by the licensed credit referenced bureaus, and the other participants, with the letter and spirit of the regulations, without imposing undue limitations to a well-functioning national credit reference system.

ROLE OF THE CENTRAL BANK

THE CENTRAL BANK AS A FACILITATOR

Given the clear benefits of credit bureaus to its mandate and objectives, the Central Bank of Kenya acts as a facilitator, working with stakeholders to implement a clear regulatory framework leading t a broad national credit reference system that provides: product innovation; a high value product with nominal unitary transaction fees; operating rules that are participant-neutral; cost sensitive procedures and rules understood by all participants; a high volume of data and reports; consumer confidentiality; transparency in transactions; data accuracy; easy error correction; reasonable consumer protection; and the flexibility to broaden participation to non financial creditor and related and other stakeholders (such as employers and landlords) activities. Product innovation by individual Credit reference bureaus should be welcomed and facilitated.

THE CENTRAL BANK AS AN HONEST BROKER

The development of a credit reference system involves fears by the stakeholders: creditors worry that their better credit customers are going to be stolen by competitors with unauthorized access to their files; data providers fear that they are going to be sued, particularly as individuals, by disgruntled customers for invasion of privacy, slander, etc., as a result of good faith participation in the provision of credit histories; customers fear that they may be black listed and that they may be affected by mistakes; subscribers to credit reports fear that they may be sued for whatever use they make of credit reports. All participants recognize the benefits of a well functioning credit information system and look to the central bank to establish and enforce a level playing field, particularly when the law gives it ownership of the Credit Reference Bureau’s database.

BALANCING CONSUMER PROTECTION AND CREDIT REFERENCE BUREAU OPERATIONS

Credit bureaus face substantial technical obstacles to obtain, screen, identify, and consolidate, massive amounts of records. The prevention of mistakes, particularly by data providers, and the handling by the credit bureaus of credit customer complaints are a significant burden. Credit individuals wrongly identified as defaulters suffer market sanctions. A balance needs to be identified that is fair to participants.

THE CENTRAL BANK AND CREDIT SCORING

The wish by creditors to rely on credit scoring for credit decisions (as compared with portfolio credit risk management) may impose unfair and arbitrary limitations to credit by individuals merged into risk groups by credit bureaus on the basis of debatable statistical analyses. Additionally, creditors relying on credit scores for credit decisions may relax or abandon the use of prudent credit principles. Since the *Banking (Credit Reference Bureau) Regulations* permit credit bureaus to ¨assess¨ the credit worthiness of credit customers, the Central Bank of Kenya needs to be especially vigilant regarding the provision and use of credit scores. Credit scores should only be allowed after the methodology used by the Credit reference bureaus (not their proprietary algorithm) is reviewed by the Central Bank of

Kenya but also, more importantly, after the proposed users receive guidance on the proper and the incorrect uses of scoring in credit decisions.

SPECIAL CENTRAL BANK OF KENYA INSTRUCTIONS ON CREDIT REFERENCE BUREAUS

To reduce many disputes without affecting the integrity of the national credit reference system, the CBK instructs licensed credit bureaus to eliminate the tracking, and the inclusion in credit reports, of arrears or unpaid fees below the equivalent of 1,000 Kenyan shillings.

The CBK is to require that it approves the data provision formats, and the credit report subscription agreements, between the Credit reference bureaus and participants. These agreements, to the maximum extent possible, are to require participants to have a copy of the required procedures, their undertaking to comply with them, and their acceptance of the right of the credit reference bureau and of the Central Bank of Kenya to conduct inspections to supervise compliance.

CONSUMER COMPLAINTS

The Central Bank of Kenya delegates to a committee the resolution by arbitration of customer complaints not solved by the credit reference bureaus. This committee includes retired Central Bank of Kenya officers and bank officers. The Central Bank of Kenya monitors and supervises the process of resolving consumer disputes and has the right to make final determination.

OFF-SITE SUPERVISION OF CREDIT REFERENCE BUREAUS

COMPLIANCE BY SUPERVISED ENTITIES

The off-site inspections by the Bank Supervision Department and by the Financial Institutions Supervision Department are to include written confirmation, signed by an authorized representative of each supervised bank or institution, to the effect that credit reference reports are:

- Obtained from which licensed credit bureaus;
- Only after the customer authorizes it in writing;
- Used for the authorized purposes; and,
- Stored as confidential information, with restricted access.

These verifications are to be communicated by the corresponding Central Bank of Kenya Inspector to the Manager of Credit Reference Bureau Supervision.

GENERAL LOG

The Inspector will keep a General Log of correspondence with licensed credit bureaus which involve or constitute Central Bank of Kenya Instructions or interpretation of Laws, Regulations, or Instructions.

The General Log is to be consulted by the Inspector before preparing an Instruction to a Credit Bureau or an interpretation of existing laws of Regulations. Such Central Bank communications to one licensed credit reference bureau will be sent to all credit bureaus.

The Inspector will write it the General Log any developments, such as Instructions or Regulations, which should be considered in the future to decide on questions or enquiries from credit bureaus.

INDIVIDUAL LOG

The Inspector is to keep an individual Log for each licensed credit reference bureau, summarizing the monthly status, indicating any reported and unsolved problems, and the action undertaken by the corresponding credit bureau.

The Inspector will note in the Individual Log whether the reported problems or incidents are isolated events or recurrent problems, and whether they represent a system-wide weakness.

If so, the inspector will note the proposed corrective solution and the date for follow up of its review, or for action.

MONTHLY REPORTS

The off-site supervision by the Central Bank of Kenya of supervised credit reference bureaus requires their submission to the Central Bank of Kenya Bank Supervision Department of the Comprehensive Monthly Report (Attachment I) which is to be submitted by the authorized representative of licensed Credit reference bureaus each month during the first week of the following month.

The *Comprehensive Monthly Report* is to include: Identification of any problems or concerns identified by the Credit Reference Bureau, or reported to it by participants, and any proposed corrective action considered.

The Inspector is to consider the effects of the reported problem or concern on the other sections of the report.

The Inspector will review whether further action by the central bank is warranted at the time. If so, the Inspector will determine if further written o telephone communication is required with the reporting credit bureau. The, the Inspector will determine the appropriate course of action, and will consult with peers in the ICT Department and with supervisors accordingly.

In particular, the Inspector will determine whether the reported problem or incident might be an early alert of misconduct or institutional weaknesses, whether of the credit bureau, of processes or Regulations, or of supervised financial institutions, that should be reported to peers and superiors.

Description of internal, participant, and third-party, data security incidents

Cyber attacks on data centers are a daily occurrence. The Inspector will consult with his peers at the ICT Department for assistance in reviewing and analyzing the data security incident, and in designing a plan of action or recommendations, if any.

As appropriate, the Inspector will inform the other licensed credit reference bureaus to check whether their data security systems and/or databases may have been compromised, and / or to improve their procedures, if necessary.

If the reported data security incident concerns a supervised financial institution o may represent a danger to any of them, the Inspector will inform the corresponding peers and supervisors.

Compliance with the use of Central Bank of Kenya-approved text of the agreements for data provision, and for subscription to credit reports

The Inspector will note any agreements reported to contain text not approved by the Central Bank, assess the importance and/or complexity of the case, and decide on the appropriate course of action, if any. The dates for follow up for full compliance, or waiver, of the requirement will be noted in the Individual Log for that credit bureau.

As required, the Inspector will consult with the CBK Legal Department for interpretation of the non conforming text, and advice on actions.

Actions, if any, undertaken by the Credit reference bureaus to ensure that all participants comply with regulations, including subscribers

The Inspector will note any course of action to be recommended to other credit bureaus.

Report that all required procedures were adhered to, with exceptions and corrections noted

The Inspector will note any course of action to be recommended.

The Inspector will note in the Individual Log whether the reported exceptions with the proposed corrective solution and the date for follow up of its review, or for action.

Report on the number of consumer complaints, presented and resolved within the required dates, and with date brackets for complaints not resolved in time

Consumer complaints are a natural condition of credit reference systems. The Inspector will monitor that fairness is provided to individuals within reasonable procedures.

The Inspector will analyze whether there are symptoms of systematic weaknesses and, if so, what the recommended course o action seems to be in order to prepare recommendations to peers and supervisors.

Listing of the name and details of regular and occasional data providers, highlighting new names since the previous report

The Inspector will scan the new data providers to enquire, as needed, on the particular circumstances of the new data provider, with particular consideration given to data accuracy, transparency, and relevance for credit references and related services.

Listing of the name and details of regular and occasional subscribers

The Inspector will scan the new subscribers to enquire, as needed, on the particular circumstances of the new purchaser, with particular consideration given to the authorized uses of credit references and related services by subscribers, including the consent of the data subjects.

The Inspector will also monitor the On-Site Inspection Reports of banks and other financial institutions prepared by peers.

The Inspector will recommend corrective action, as warranted.

Fees charged

The Inspector will monitor fees charged for services given the policy of the Central Bank of Kenya to allow the market to decide the fees whenever feasible, but to monitor them to avoid collusion or distortions.

Breakdown of the services provided by credit reference bureaus to subscribers

The Inspector will carefully monitor the various services provided by the different credit bureaus for compliance with Regulations, and will contact the credit bureaus, as required, to understand new products and services and their uses, taking care not to inadvertently reveal one credit bureau´s industrial secrets to other credit bureaus.

Specific report on the participants and volume of any service to assess the credit worthiness of customers

The Inspector will monitor that credit scoring for credit decisions does not impose unfair or arbitrary limitations to credit by individuals merged into risk groups by credit bureaus on the basis of unproven statistical analyses.

Additionally, the Inspector will monitor through peer Inspectors of financial institutions that creditors relying on credit scores for credit decisions do not may relax or abandon the use of prudent credit principles.

The Inspector will monitor that the methodology to generate credit scores be reviewed by the Central Bank of Kenya, and that the proposed users receive guidance from the credit bureau on the proper and the incorrect uses of credit scoring in credit decisions.

Certification from the credit bureau that its data providers provide all relevant credit records, noting any exemptions with reasons and proposed actions, if any

It is normal for creditors and other data providers to withhold records having insufficient identifiable fields or having inaccurate data. The Inspector will monitor that data providers, particularly supervised institutions, do not withhold records for unjustified reasons, such as trying to protect related parties.

Certification from the credit bureau that its data center still meets the requirements for licensing, noting any exemptions and planned actions

The Inspector will monitor that any deviations from the required criteria for approval of the data center are not serious, and that a credible upgrade plan to meet specifications is under way with an acceptable completion date.   The Inspector will note in the Individual Log the particular exemptions and the expected date for compliance.

Copy of external and internal auditors´ reports generated during the period, including any technical inspections of the data center or systems

The inspector will review any inspection or auditor reports for indication of any violations of laws, Regulations, or Instructions, and will take appropriate corrective action.

ON-SITE EXAMINATION OF CREDIT REFERENCE BUREAUS

The Inspector will coordinate with its counterpart at the ICT department. Both will review the file for the licensed credit bureau, particularly the previous on-site examination report, read the Monthly Reports since the last examination, and read the Individual Log for the credit bureau to be examined, noting the previous physical inspection reports, including the inspection for granting the license.

In addition the Inspector will highlight sector wide concerns that should be included in the examination.

The ICT Department counterpart Inspector will also note particular areas to be examined in light of recent trends or incidents related to information security.

The ICT Department counterpart Inspector will prepare a check list for ICT technical examination using the *Sample Best Practices for Examination Procedures of Information Security*, attached in Annex I

Together, the team of Inspectors will determine the scope of the joint examination and the dates and duration of same. The Inspectors will schedule the joint examination with the credit reference bureau, indicating the documents and staff (and any external expert inspectors or auditors), indicating the corresponding dates in which each should be present or available.

The on-site inspection by the CBK of banks and other financial institutions is to include verification that credit reports are: obtained only after the customer authorizes it in writing; used for the authorized purposes; and, stored as confidential information with restricted access.

Results of these verifications are to be communicated by the CBK Bank Inspectors and by the Other Financial Institution Inspectors to the CBK manager in charge of credit bureau supervision.

Specific tasks of the examination include: Determine that the primary and alternate premises are still suitable for operations.

The objective of the examination is to ensure that promises have separate areas with access restricted to authorized persons and with established and acceptable security procedures known and followed.

Verify that the Monthly Reports submitted to the Central Bank of Kenya by a credit reference bureau is validated by the internal records of the credit reference bureau

The objective of this part of the on-site examination is to inspect that company records to substantiate the veracity and validity of reports sent to the CBK every month by the credit bureau.

The examiner will conduct spot checks of each point to be reported monthly against a representative number of company documents and correspondence, and through separate interviews of management, staff, and also of external auditors and technical inspectors.

Verify that the credit reference bureau´s systems, procedures, and facilities, are valid

The joint examination team will check the written policies, processes, and operational procedures are updated, consistent with current practices, and know and followed by the corresponding levels of staff.

The examination of information security procedures will follow the check list prepared by the ICT Department Inspector, who will lead this part of the examination.

Verify that the credit reference bureau staffers know and follow their assigned specified procedures

Trough selective interviews and observations of procedures with managers and staff at various levels, the Inspector will verify that assigned credit bureau staffers know the operating policies and procedures for their assigned tasks, and follow them.

The Examiner will note any material discrepancies between observed practices and written procedures.

Verify that the security and control protocols are relevant, and implemented

Trough selective interviews and observations of procedures with managers and staff at appropriate levels, the Examiner will verify that assigned credit bureau staffers know and follow the respective security and control protocols, that those protocols are current and updated, and that the protocols are still relevant, particularly in light of any security incidents at an credit bureau.

The Examiner will enquire as to any ideas for improvement and will note any material discrepancies between observed practices and written security protocols.

Verify that the protocols for updating and maintaining information are still valid and that are followed

The Examiner team will verify that information is processed, stored, updated, maintained and used in accordance with established policies and protocols. In particular, the Examiner will consider whether the information updating and maintaining protocols are still valid.

The Examiner will verify that old and irrelevant or faulty information to be used for credit reports is segregated from the database used to generate credit reports.

Verify that the Business Continuity provisions are in place and are still valid

The Examiners will request a demonstration by the credit bureau simulating an emergency scenario requiring that Business Continuity provisions be implemented.

The demonstration may be substituted by a recent technical stress simulation test conducted by an independent testing agent acceptable to the Central Bank.

The Examiners will discuss with management any practical ideas for improving the capacity of the credit bureau to maintain required Business Continuity standards.

Verify that data providers and subscribers of credit reports are aware and follow the required procedures

The Examiners will discuss with the management of the credit bureau any cases discovered by their peer CBK bank Inspectors, and / or CBK Inspectors of other financial institutions, where staffers of the institutions involved in data provider or credit report functions are unaware of, or do not follow, required procedures.

The Examiners will analyze any records of training or due diligence visits by the credit bureau to their data providers and subscribers.

Verify that the credit reference bureau has on file signed agreements for each data provider and subscriber

The Examiners will confirm in the company files if the credit bureau has on file signed agreements for each active data provider and/or subscriber.

The Examiners will discuss with the management of the credit bureau any cases discovered by their peer CBK bank Inspectors, and / or CBK Inspectors of other financial institutions, where those institutions do not have in their files an agreement with the credit bureau.

Verify that consumer complaints are handled as required and that logs and records for resolution of complaints are maintained and updated

The Examiners will thoroughly discuss with management the current policies, processes, and practices for resolving consumer complaints, highlighting any ideas for improvement.

The Examiners will inspect the files and the in house system for resolution of consumer complaints, and will interview assigned staff.

The Examiners will note any discrepancies between the Monthly Reports and observed records.

The Examiners will discuss with the management of the credit bureau any cases discovered by their peer CBK bank Inspectors, and / or CBK Inspectors of other financial institutions, where those institutions´ records on consumer complaints on credit reports differ from the credit bureaus´

Verify that audit trails in the system are valid

The Examiners, in coordination with the Chief Information Officer of the credit bureau, will use the relevant aspects of Annex I to conduct a thorough joint examination of the system and protocols for audit trails.

Verify that the protocols for internal and external user access, including passwords and logs, are adhered to

The Examiners, in coordination with the Chief Information Officer of the credit bureau, will use the relevant aspects of Annex I to conduct a thorough joint examination of the system and protocols for internal and external user access.

The Examiners will thoroughly discuss with management the current policies, processes, and practices for controlling internal and external access, highlighting any ideas for improvement, in light of any known security breaches.

Verify that any service to assess the credit worthiness of customers is based on sound statistical methodology

The Examiners will review contracts, agreements, manuals, and billing records, as well as the system applications, to determine that any statistical modeling of the database to determine generic of creditor specific credit scoring methods does not unduly affect a class of persons and is in compliance with CBK Regulations and Instructions.

Verify that information sharing restrictions are adhered **to**

The Examiner will review written policies and systems to verify that any restrictions imposed by Law, Regulation or by the Central Bank, such as the limitations between credit reference reporting and credit collections are observed.

Communicate preliminary findings and discuss corrective action

The Inspector will review the preliminary conclusions with the Chief Information Officer and with the Chief Executive Officer regarding any violations of Law, Regulations, or Instructions.

The Inspector will discuss in detail any significant issues deserving inclusion as items requiring attention, or as recommendations, in the Report of Examination.

The inspector will discuss the draft findings with the management of the credit bureau and obtain from them comments on their proposed corrective action for significant deficiencies.

After returning to the Central Bank, the Inspectors will draft joint conclusions in an internal memo to their supervisors that provides comments for all relevant sections of the Report of Examination and that serves as guidance to future Inspectors.

The inspectors will organize their work papers to ensure clear support for each significant finding, arranged by examination objective.

ANNEX I

SAMPLE BEST PRACTICES FOR EXAMINATION PROCEDURES OF INFORMATION SECURITY OF LICENSED CREDIT REFERENCE BUREAUS EXAMINATION OBJECTIVE

Assess the quantity of risk and the effectiveness of the institution's risk management processes as they relate to the security measures instituted to ensure confidentiality, integrity, and availability of information and to instill accountability for actions taken on the institution's systems. The objectives and procedures are divided into Tier 1 and Tier II:

- Tier I assesses an institution's process for identifying and managing risks.
- Tier II provides additional verification where risk warrants it.

Tier I and Tier II are intended to be a tool set Inspectors will use when selecting examination procedures for their particular examination. Inspectors should use these procedures as necessary to support examination objectives.

Tier I Procedures

Objective 1: Determine the appropriate scope for the examination

1. Review past reports for outstanding issues or previous problems.
   a. Regulatory reports of examination
   b. Internal and external audit reports
   c. Independent security tests
   d. Regulatory, audit, and security reports from service providers

2. Review management's response to issues arising at the last examination.
   a. Adequacy and timing of corrective action
   b. Resolution of root causes rather than just specific issues
   c. Existence of any outstanding issues

3. Interview management and review examination information to identify changes to the technology infrastructure or new products and services that might increase the institution's risk from information security issues.
   a. Products or services delivered to either internal or external users
   b. Network topology including changes to configuration or components
   c. Hardware and software listings
   d. Loss or addition of key personnel
   e. Technology service providers and software vendor listings
   f. Changes to internal business processes
   g. Key management changes
   h. Internal reorganizations

4. Determine the existence of new threats and vulnerabilities to the institution's information security. Consider
   a. Changes in technology employed by the institution
   b. Threats identified by institution staff

c. Known threats identified by information sharing and analysis organizations and other non-profit and commercial organizations
d. Vulnerabilities raised in security testing reports

QUANITY OF RISK

Objective 2: Determine the complexity of the institution's information security environment

1. Review the degree of reliance on service providers for information processing and technology support including security management. Review evidence that service providers of information processing and technology know and comply with CBK Regulations.

2. Identify unique products and services and any required third-party access requirements.

3. Determine the extent of network connectivity internally and externally, and the boundaries and functions of security domains.

4. Identify the systems that have recently undergone significant change, such as new hardware, software, configurations, and connectivity. Correlate the changed systems with the business processes they support, the extent of customer data available to those processes, and the role of those processes in funds transfers.

5. Evaluate management's ability to control security risks given the frequency of changes to the computing environment.

6. Evaluate security maintenance requirements and extent of historical security issues with installed hardware/software.

7. Identify whether external standards are used as a basis for the security program, and the extent to which management tailors the standards to the financial institutions' specific circumstances.

8. Determine the size and quality of the institution's security staff. Consider
   a. Appropriate security training and certification
   b. Adequacy of staffing levels and impact of any turnover
   c. Extent of background investigations
   d. Available time to perform security responsibilities

QUALITY OF RISK MANAGEMENT

Objective 3: Determine the adequacy of the risk assessment process

1. Review the risk assessment to determine whether the institution has characterized its system properly and assessed the risks to information assets.
   a. Identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to customer non-public information as well as the risks to the institution
   b. Identified all reasonably foreseeable threats to the financial institution assets
   c. Analyzed its technical and organizational vulnerabilities, and
   d. Considered the potential effect of a security breach on customers as well as the institution

2. Determine whether the risk assessment provides adequate support for the security strategy, controls, and monitoring that the financial institution has implemented.

3. Evaluate the risk assessment process for the effectiveness of the following key practices:
   a. Multidisciplinary and knowledge-based approach
   b. Systematic and centrally controlled
   c. Integrated process
   d. Accountable activities
   e. Documented
   f. Knowledge enhancing
   g. Regularly updated

4. Identify whether the institution effectively updates the risk assessment prior to making system changes, implementing new products or services, or confronting new external conditions that would affect the risk analysis. Identify whether, in the absence of the above factors, the risk assessment is reviewed at least once a year.

Objective 4: Evaluate the adequacy of security policies and standards relative to the risk to the institution

1. Review security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution. If policy validation is necessary, consider performing Tier II procedures.
   a. Authentication and Authorization
      (i) Acceptable-use policy that dictates the appropriate use of the institution’s technology including hardware, software, networks, and telecommunications
      (ii) Administration of access rights at enrollment, when duties change, and at employee separation
      (iii)Appropriate authentication mechanisms including token-based systems, digital certificates, or biometric controls and related enrollment and maintenance processes as well as database security.
   b. Network Access
      (i) Security domains
      (ii) Perimeter protections including firewalls, malicious code prevention, outbound filtering, and security monitoring

(iii) Appropriate application access controls

(iv) Remote access controls including wireless, VPN, modems, and Internet-based

c. Host Systems
   (i) Secure configuration (hardening)
   (ii) Operating system access
   (iii) Application access and configuration
   (iv) Malicious code prevention
   (v) Logging
   (vi) Monitoring and updating
d. User Equipment
   (i) Secure configuration (hardening)
   (ii) Operating system access
   (iii) Application access and configuration
   (iv) Malicious code prevention
   (v) Logging
   (vi) Monitoring and updating
e. Physical controls over access to hardware, software, storage media, paper records, and facilities
f. Encryption controls
g. Malicious code prevention
h. Software development and acquisition, including processes that evaluate the security features and software trustworthiness of code being developed or acquired, as well as change control and configuration management
i. Personnel security
j. Media handling procedures and restrictions, including procedures for securing, transmitting and disposing of paper and electronic information
k. Service provider oversight
l. Business continuity
m. Insurance

2. Evaluate the policies and standards against the following key actions.
   a. Implementing through ordinary means, such as system administration procedures and acceptable-use policies
   b. Enforcing with security tools and sanctions
   c. Delineating the areas of responsibility for users, administrators, and managers
   d. Communicating in a clear, understandable manner to all concerned
   e. Obtaining employee certification that they have read and understood the policy
   f. Providing flexibility to address changes in the environment
   g. Conducting annually a review and approval by the board of directors

Objective 5: Evaluate the security-related controls embedded in vendor management

1. Evaluate the sufficiency of security-related due diligence in service provider research and selection.

2. Evaluate the adequacy of contractual assurances regarding security responsibilities, controls, and reporting.

3. Evaluate the appropriateness of nondisclosure agreements regarding the institution’s systems and data.

4. Determine that the scope, completeness, frequency, and timeliness of third-party audits and tests of the service provider's security are supported by the financial institution's risk assessment.

5. Evaluate the adequacy of incident response policies and contractual notification requirements in light of the risk of the outsourced activity.

Objective 6: Determine the adequacy of security monitoring

1. Obtain an understanding of the institution's monitoring plans and activities, including both activity monitoring and condition monitoring.

2. Identify the organizational unit and personnel responsible for performing the functions of a security response center.

3. Evaluate the adequacy of information used by the security response center. Information should include external information on threats and vulnerabilities and internal information related to controls and activities.

4. Obtain and evaluate the policies governing security response center functions, including monitoring, classification, escalation, and reporting.

5. Evaluate the institution's monitoring plans for appropriateness given the risks of the institution's environment.

6. Where metrics are used, evaluate the standards used for measurement, the information measures and repeatability of measured processes, and appropriateness of the measurement scope.

7. Ensure that the institution utilizes sufficient expertise to perform its monitoring and testing.

8. For independent tests, evaluate the degree of independence between the persons testing security from the persons administering security.

9. Determine the timeliness of identification of vulnerabilities and anomalies, and evaluate the adequacy and timing of corrective action.

10. Evaluate the institution's policies and program for responding to unauthorized access to customer information.

11. If the institution experienced unauthorized access to sensitive customer information, determine:
    a. Conducted a prompt investigation to determine the likelihood the information accessed has been or will be misused
    b. Notified customers when the investigation determined misuse of sensitive customer information has occurred or is reasonably possible
    c. Delivered notification to customers, when warranted, by means the customer can reasonably be expected to receive, for example, by telephone, mail, or electronic mail

    d. Appropriately notified the CBK

Objective 7: Evaluate the effectiveness of enterprise-wide security administration

1. Review board and committee minutes and reports to determine the level of senior management support of and commitment to security.

2. Determine whether management and department heads are adequately trained and sufficiently accountable for the security of their personnel, information, and systems.

3. Review security guidance and training provided to ensure awareness among employees and contractors, including annual certification that personnel understand their responsibilities.

4. Determine whether security responsibilities are appropriately apportioned among senior management, front-line management, IT staff, information security professionals, and other staff, recognizing that some roles must be independent from others.

5. Determine whether the individual or department responsible for ensuring compliance with security policies has sufficient position and authority within the organization to implement the corrective action.

6. Evaluate the process used to monitor and enforce policy compliance (e.g., granting and revocation of user rights).

7. Evaluate the adequacy of automated tools to support secure configuration management, security monitoring, policy monitoring, enforcement, and reporting.

8. Evaluate management's ability to effectively control the pace of change to its environment, including the process used to gain assurance that changes to be made will not pose undue risk in a production environment. Consider the definition of security requirements for the changes, appropriateness of staff training, quality of testing, and post-change monitoring.

9. Evaluate coordination of incident response policies and contractual notification requirements.

CONCLUSIONS

Objective 8: Discuss corrective action and communicate findings

1. Determine the need to proceed to Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. Review your preliminary conclusions with the Chief Information Officer regarding
    a. Violations of law, rulings, regulations
    b. Significant issues warranting inclusion as matters requiring attention or recommendations in the Report of Examination
    c. Potential impact of your conclusions on composite or component IT ratings
    d. Potential impact of your conclusions on the institution’s risk assessment

3. Discuss your findings with management and obtain proposed corrective action for significant deficiencies.

4. Document your conclusions in a memo to the Chief Information Officer that provides report-ready comments for all relevant sections of the Report of Examination and guidance to future Inspectors

5. Organize your work papers to ensure clear support for significant findings by examination objective.

Tier II Objectives and Procedures

The Tier II examination procedures for information security provide additional verification procedures to evaluate the effectiveness of, and identify potential root causes for weaknesses in a credit bureau’s security program. These procedures are designed to assist in achieving examination objectives and may be used in their entirety or selectively, depending upon the scope of the examination and the need for additional verification. For instance, if additional verification is necessary for firewall practices, the Inspector may find it necessary to select some of the procedures from the authentication, network security, host security, and physical security areas to create a customized examination procedure.

The procedures provided below should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risks facing the institution's information system. Thus, the controls necessary for any single credit bureau or any given area of a given institution may differ from the specifics that can be inferred from the following procedures.

AUTHENTICATION AND ASSESS CONTROLS

Access Rights Administration

1. Evaluate the adequacy of policies and procedures for authentication and access controls to manage effectively the risks to the financial institution.
   a. 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
   b. Review processes that assign rights and privileges and ensure that they take into account and provide for adequate segregation of duties
   c. 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
   d. Ensure that access to operating systems is based on either a need-to-use or an event-by-event basis

2. Determine whether the user registration and enrollment process.
   a. Uniquely identifies the use
   b. Verifies the need to use the system according to appropriate policy
   c. Enforces a unique user ID
   d. Assigns and records the proper security attributes (e.g., authorization)

   e. Enforces the assignment or selection of an authenticator that agrees with the security policy
   f. Securely distributes any initial shared secret authenticator or token
   g. Obtains acknowledgement from the user of acceptance of the terms of use

3. Determine whether employee's levels of online access (blocked, read-only, update, override, etc.) match current job responsibilities.

4. Determine that administrator or root privilege access is appropriately monitored, where appropriate.
   a. 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.

5. Evaluate the effectiveness and timeliness with which changes in access control privileges are implemented and the effectiveness of supporting policies and procedures.
   a. Review procedures and controls in place and determine whether access control privileges are promptly eliminated when they are no longer needed and include former employees and temporary access for remote access and contract workers in the review
   b. Assess the procedures and controls in place to change, when appropriate, access control privileges (e.g., changes in job responsibility and promotion)
   c. Determine whether access rights expire after a predetermined period of inactivity
   d. 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

6. 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.
7. Compare the access control rules establishment and assignment processes to the access control policy for consistency.

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

Authentication

1. Determine whether the credit bureau has removed or reset default profiles and passwords from new systems and equipment.

2. Determine whether access to system administrator level is adequately controlled and monitored.

3. Evaluate whether the authentication method selected and implemented is appropriately supported by a risk assessment.

4. 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.
   a. Confidentiality of passwords and shared secrets (whether only known to the employee/customer)
   b. Maintenance of confidentiality through reset procedures
   c. 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)
   d. 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)
   e. The strength of shared secret authentication mechanisms
   f. Restrictions on duplicate shared secrets among users (no restrictions should exist)
   g. The extent of authorized access (e.g., privileged access, single sign-on systems)

   5. Determine whether all authenticators (e.g., passwords, shared secrets) are protected while in storage and during transmission to prevent disclosure.
   a. Identify processes and areas where authentication information may be available in clear text and evaluate the effectiveness of compensating risk management controls
   b. 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

6. 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.

7. 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.

8. 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.

9. Determine whether adequate controls exist to protect against replay attacks and hijacking.

10. 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.

11. Determine whether PKI-based authentication mechanisms.
    a. Securely issue and update keys

- b. Securely unlock the secret key
- c. Provide for expiration of keys at an appropriate time period
- d. Ensure the certificate is valid before acceptance
- e. Update the list of revoked certificates at an appropriate frequency
- f. Employ appropriate measures to protect private and root keys
- g. Appropriately log use of the root key

12. Determine that biometric systems
    - a. Have an adequately strong and reliable enrollment process
    - b. Adequately protect against the presentation of forged credentials (e.g. address replay attacks)
    - c. Are appropriately tuned for false accepts/false rejects.

13. Determine whether appropriate device and session authentication takes place, particularly for remote and wireless machines.

14. Review authenticator reissuance and reset procedures. Determine whether controls adequately mitigate risks from
    - a. Social engineering
    - b. Errors in the identification of the user
    - c. Inability to re-issue on a large scale in the event of a mass compromise

NETWORK SECURITY

1. Evaluate the adequacy and accuracy of the network architecture.
    - a. Obtain a schematic overview of the financial institution's network architecture
    - b. Review procedures for maintaining current information, including inventory reporting of how new hardware are added and old hardware is removed
    - c. Review audit and security reports that assess the accuracy of network architecture schematics and identify unreported systems

2. 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.
    - a. Review network architecture policies and procedures to establish new, or change existing, network connections and equipment
    - b. Identify controls used to prevent unauthorized deployment of network connections and equipment
    - c. Review the effectiveness and timeliness of controls used to prevent and report unauthorized network connections and equipment

3. Evaluate controls over the management of remote equipment.

4. Determine whether effective procedures and practices are in place to secure network services, utilities, and diagnostic ports, consistent with the overall risk assessment.

5. Determine whether external servers are appropriately isolated through placement in separate or ¨demilitarized zones (DMZs)¨, with supporting servers on DMZs separate from external networks, public servers, and internal networks.

6. Determine whether appropriate segregation exists between the responsibility for networks and the responsibility for computer operations.

7. 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.

8. Determine that, where appropriate, authenticated users and devices are limited in their ability to access system resources and to initiate transactions.

9. Evaluate the appropriateness of technical controls mediating access between security domains.
   a. Firewall topology and architecture
   b. Type(s) of firewall(s) being utilized
   c. Physical placement of firewall components
   d. Monitoring of firewall traffic
   e. Firewall updatingResponsibility for monitoring and updating firewall policy
   f. Placement and monitoring of network monitoring and protection devices, including intrusion detection system (IDS) and intrusion prevention system (IPS) functionality
   g. Contingency planning

10. Determine whether firewall and routing controls are in place and updated as needs warrant.
    a. Identify personnel responsible for defining and setting firewall rule sets and routing controls
    b. Review procedures for updating and changing rule sets and routing controls
    c. Confirm that the rule set 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
    d. Confirm that network mapping through the firewall is disabled
    e. Confirm that network address translation (NAT) and split DNS are used to hide internal names and addresses from external users
    f. Confirm that malicious code is effectively filtered
    g. Confirm that firewalls are backed up to external media, and not to servers on protected networks
    h. Determine that firewalls and routers are subject to appropriate and functioning host controls
    i. Determine that firewalls and routers are securely administered
    j. Confirm that routing tables are regularly reviewed for appropriateness on a schedule commensurate with risk

11. Determine whether network-based IDSs are properly coordinated with firewalls (see "Security Monitoring" procedures).

12. 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 additionally, determine that adequate clock synchronization takes place.

13. 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.

14. Determine whether appropriate filtering occurs for spoofed addresses, both within the network and at external connections, covering network ingress and egress.

15. Determine whether appropriate controls exist over the confidentiality and integrity of data transmitted over the network (e.g. encryption, parity checks, message authentication).

16. Determine whether appropriate notification is made of requirements for authorized use, through banners or other means.

17. Determine whether remote access devices and network access points for remote equipment are appropriately controlled.
    a. Remote access is disabled by default, and enabled only by management authorization.
    b. Management authorization is required for each user who accesses sensitive components or data remotely
    c. Authentication is of appropriate strength (e.g., two-factor for sensitive components)
    d. Modems are authorized, configured, and managed to appropriately mitigate risks
    e. Appropriate logging and monitoring takes place
    f. Remote access devices are appropriately secured and controlled by the institution

18. Determine whether an appropriate archive of boot disks, distribution media, and security patches exists

19. Evaluate the appropriateness of techniques that detect and prevent the spread of malicious code across the network.

HOST SECURITY

1. Determine whether hosts are hardened through the removal of unnecessary software 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.

2. Determine whether the configuration minimizes the functionality of programs, scripts, and plug-ins to what is necessary and justifiable.

3. Determine whether adequate processes exist to apply host security updates, such as patches and anti-virus signatures, and that such updating takes place.

4. Determine whether new hosts are prepared according to documented procedures for secure configuration or replication, and that vulnerability testing takes place prior to deployment.

5. Determine whether remotely configurable hosts are configured for secure remote administration.

6. 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.

7. Determine whether access to utilities on the host are appropriately restricted and monitored.

8. 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.”)

9. 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.

10. Determine whether vulnerability testing takes place after each configuration change.

11. Determine whether appropriate notification is made of authorized use, through banners or other means.

12. Determine whether authoritative copies of host configuration and public server content are maintained off line.

13. Determine whether an appropriate archive of boot disks, distribution media, and security patches exists.

14. 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)

1. 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.

2. Determine whether user equipment is configured either for secure remote administration or for no remote administration.

3. Determine whether adequate inspection for, and removal of, unauthorized hardware and software takes place.

4. 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.

5. 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.

6. Determine whether appropriate user equipment is deactivated after a period of inactivity through screen saver passwords, server time-outs, powering down or other means.

7. Determine whether systems are appropriately protected against malicious software such as Trojan horses, viruses, and worms.

PHYSICAL SECURITY

1. Determine whether physical security for information technology assets is coordinated with other security functions.

2. Determine whether sensitive data in both electronic and paper form is adequately controlled physically through creation, processing, storage, maintenance, and disposal.
   a. Authorization for physical access to critical or sensitive information-processing facilities is granted according to an appropriate process
   b. Authorizations are enforceable by appropriate preventive, detective, and corrective controls
   c. Authorizations can be revoked in a practical and timely manner

3. 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

1. Determine whether the credit bureau 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.

2. Determine whether the institution includes in its terms and conditions of employment the employee's responsibilities for information security.

3. Determine whether the institution requires personnel with authority to access customer information and confidential institution information to sign and abide by confidentiality agreements.

4. Determine whether the institution provides to its employees appropriate security training covering the institution's policies and procedures, on an appropriate frequency and that institution employees certify periodically as to their understanding and awareness of the policy and procedures.

5. Determine whether employees have an available and reliable mechanism to promptly report security incidents, weaknesses, and software malfunctions.

6. Determine whether an appropriate disciplinary process for security violations exists and is functioning.

APPLICATION SECURITY

1. Determine whether software storage, including program source, object libraries, and load modules, are appropriately secured against unauthorized access.

2. Determine whether user input is validated appropriately (e.g. character set, length, etc).

3. Determine whether appropriate message authentication takes place.

4. Determine whether access to sensitive information and processes require appropriate authentication and verification of authorized use before access is granted.

5. Determine whether re-establishment of any session after interruption requires normal user identification, authentication, and authorization.

6. Determine whether appropriate warning banners are displayed when applications are accessed.

7. Determine whether appropriate logs are maintained and available to support incident detection and response efforts.

SOFTWARE DEVELOPMENT AND AQUISITION

1. Inquire about how security control requirements are determined for software, whether internally developed or acquired from a vendor.

2. Determine whether management explicitly follows a recognized security standard development process, or adheres to widely recognized industry standards.

3. Determine whether the group or individual establishing security control requirements has appropriate credentials, background, and/or training.

4. 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.

5. Evaluate whether the software contains appropriate authentication and encryption.

6. Evaluate the adequacy of the change control process.

7. Evaluate the appropriateness of software libraries and their access controls.

8. Inquire about the method used to test the newly developed or acquired software for vulnerabilities.
   a. For manual source code reviews, inquire about standards used, the capabilities of the reviewers, and the results of the reviews
   b. If source code reviews are not performed, inquire about alternate actions taken to test the software for covert channels, backdoors, and other security issues

c. 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-level risk

9. Evaluate the process used to ascertain software trustworthiness. Include in the evaluation management's consideration of the:
   a. Development process
      (i) Establishment of security requirements
      (ii) Establishment of acceptance criteria
      (iii)Use of secure coding standards
      (iv)Compliance with security requirements
      (v) Background checks on employees
      (vi)Code development and testing processes
      (vii) Signed non-disclosure agreements
      (viii) Restrictions on developer access to production source code
      (ix)Physical security over developer work areas
   b. Source code review
      (i) Automated reviews
      (ii) Manual reviews
   c. Vendor or developer history and reputation
      (i) Vulnerability history
      (ii) Timeliness, thoroughness, and candidness of the response to security issues
      (iii)Quality and functionality of security patches

1. Evaluate the appropriateness of management's response to assessments of software trustworthiness.
   a. Host and network control evaluation
   b. Additional host and network controls

BUSINESS CONTINUITY – SECURITY

1. 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.
   a. Review the risk assessment to identify key control points in a data set's life cycle
   b. Verify controls are in place consistent with the level of risk presented

2. Determine whether substitute processing facilities and systems undergo similar testing as production facilities and systems.

3. 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.

4. Determine whether the security monitoring and intrusion response plan considers the resource availability and facility and systems changes that may exist when substitute facilities are placed in use.

5. Evaluate the procedure for granting temporary access to personnel during the implementation of contingency plans.

6. 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. (If an employee is permanently assigned access credentials to fill in for another employee who is on vacation or out the office, this assignment would be a primary job responsibility.)

SERVICE PROVIDER OVERSIGHT SECURITY

1. Determine whether contracts contain security requirements that at least meet the objectives of the contract guidelines and contain nondisclosure language regarding specific requirements.

2. Determine whether the credit bureau has assessed the service provider's ability to meet contractual security requirements.

3. Determine whether appropriate controls exist over the substitution of personnel on the institution's projects and services.

4. Determine whether appropriate security testing is required and performed on any code, system, or service delivered under the contract.

5. Determine whether appropriate reporting of security incidents is required under the contract.

6. Determine whether institution oversight of third-party provider security controls is adequate.

7. Determine whether any third party provider access to the institution's system is controlled according to "Authentication and Access Controls" and "Network Security" procedures.

8. Determine whether the contract requires secure remote communications, as appropriate.

9. 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.

10. Determine whether the third party service provider participates in an appropriate industry security group.

ENCRYPTION

1. Review the information security risk assessment and identify those items and areas classified as requiring encryption.

2. Evaluate the appropriateness of the criteria used to select the type of encryption/cryptographic algorithms.

    a. 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
    b. Note the basis for choosing key sizes (e.g., 40-bit, 128-bit) and key space
    c. Identify management's understanding of cryptography and expectations of how it will be used to protect data.

3. Determine whether cryptographic key controls are adequate.
    a. Identify where cryptographic keys are stored
    b. Review security where keys are stored and when they are used (e.g., in a hardware module)
    c. Review cryptographic key distribution mechanisms to secure the keys against unauthorized disclosure, theft, and diversion
    d. Verify that two persons are required for a cryptographic key to be used, when appropriate
    e. Review audit and security reports that review the adequacy of cryptographic key controls.

4. Determine whether adequate provision is made for different cryptographic keys for different uses and data.

5. Determine whether cryptographic keys expire and are replaced at appropriate time intervals.

6. Determine whether appropriate provisions are made for the recovery of data should a key be unusable.

7. Determine whether cryptographic keys are destroyed in a secure manner when they are no longer required.

DATA SECURITY

1. Obtain an understanding of the data security strategy.
    a. Identify the credit bureaus's approach to protecting data (e.g., protect all data similarly, protect data based upon risk of loss)
    b. 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
    c. Consider whether policies and procedures address the protections for data that is sent outside the institution
    d. Identify processes to periodically review data sensitivity and update corresponding risk assessments

2. Verify that data is protected consistent with the financial institution's risk assessment.
    a. 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
    b. Consider data security controls in effect at key stages such as data creation/acquisition, storage, transmission, maintenance, and destruction

    c. Review audit and security review reports that summarize if data is protected consistent with the risk assessment

3. Determine whether individual and group access to data is based on business needs.

4. 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

1. Identify the monitoring performed to identify non-compliance with institution security policies and potential intrusions.
    a. Review the schematic of the information technology systems for common security monitoring devices
    b. Review security procedures for report monitoring to identify unauthorized or unusual activities
    c. Review management’s self-assessment and independent testing activities and plans

2. Determine whether users are appropriately notified regarding security monitoring.

3. Determine whether the activity monitoring sensors identified as necessary in the risk assessment process are properly installed and configured at appropriate locations.

4. Determine whether an appropriate firewall rule set and routing controls are in place and updated as needs warrant.
    a. Identify personnel responsible for defining and setting firewall rule sets and routing controls
    b. Review procedures for updating and changing rule sets and routing controls
    c. Determine that appropriate filtering occurs for spoofed addresses, both within the network and at external connections, covering network entry and exit
5. 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.

6. 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.

7. Determine whether logs are appropriately centralized and normalized, and that controls are in place and functioning to prevent time gaps in logging.

8. 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.

9. Determine whether appropriate detection capabilities exist.
    a. Network related anomalies, including
        (i) Blocked outbound traffic

(ii) Unusual communications, including communicating hosts, times of day, protocols, and other header-related anomalies
(iii)Unusual or malicious packet payloads

b. Host-related anomalies, including
(i) System resource usage and anomalies
(ii) User related anomalies
(iii)Operating and tool configuration anomalies
(iv)File and data integrity problems
(v) Anti-virus, anti-spyware, and other malware identification alerts
(vi)Unauthorized access
(vii) Privileged access

10. Evaluate the institution’s self-assessment plan and activities.
    a. Policies and procedures conformance
    b. Service provider oversight
    c. Vulnerability scanning
    d. Configuration verification
    e. Information storage
    f. Risk assessment and monitoring plan review
    g. Test reviews

11. Evaluate the use of metrics to measure
    a. Security policy implementation
    b. Security service delivery effectiveness and efficiency
    c. Security event impact on business process

12. Evaluate independent tests, including penetration tests, audits, and assessments.
    a. Personnel
    b. Scope
    c. Controls over data integrity, confidentiality, and availability
    d. Confidentiality of test plans and data
    e. Frequency

13. Determine that the functions of a security response center are appropriately governed by implemented policies.
    a. Monitoring
    b. Classification
    c. Escalation
    d. Reporting
    e. Intrusion declaration

14. Determine whether an intrusion response team.
    a. Contains appropriate membership
    b. Is available at all times
    c. Has appropriate training to investigate and report findings
    d. Has access to back-up data and systems, an inventory of all approved hardware and software, and monitored access to systems (as appropriate)
    e. Has appropriate authority and timely access to decision makers for actions that require higher approvals.

  f. Have procedures for submitting appropriate incidents to the CBK and to the credit reference industry

15. Evaluate the appropriateness of the security policy in addressing the review of compromised systems.
    a. Documentation of the roles, responsibilities and authority of employees and contractors
    b. Conditions for the examination and analysis of data, systems, and networks

16. 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.

17. Determine whether the information disclosure policy addresses the appropriate regulatory reporting requirements.

18. 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.

19. 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.

20. 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.

21. Determine whether response policies and training appropriately address unauthorized disclosures of customer information.
    a. Identifying the customer information and customers effected
    b. Protecting those customers through monitoring, closing, or freezing accounts
    c. Notifying customers when warranted
    d. Appropriately notifying its primary federal regulator

22. Determine whether an effective process exists to respond in an appropriate and timely manner to newly discovered vulnerabilities. Consider
    a. Assignment of responsibility
    b. Prioritization of work to be performed
    c. Appropriate funding
    d. Monitoring
    e. Follow-up activities