Business

Remote Deposit Capture

Risk Self-Assessment

Table of Contents

BACKGROUND

The Federal Financial Institutions Examination Council (FFIEC) published “Risk Management of Remote Deposit Capture” on January 14, 2009. The guidance was issued “for examiners, financial institutions, and technology service providers to identify risks, evaluate controls and assess risk management practices related to remote deposit capture systems (RDCS).” All U.S. financial institutions and their Customers/Customers will be governed by these guidelines.

The FFIEC explained the need for the Guidelines, “Compliance of all institutions is important because of the nature of Remote Deposit Capture technology and its adaptability for illegal activities. For years, U.S. financial institutions have been required to qualify Customers and Customers, in accordance with the Bank Secrecy Act, Patriot Act and Gramm, Leach, Bliley Act, collectively (The Rules) to preserve the stability of the financial industry.

RDCS enables customers to make deposits from their homes or businesses instead of taking the deposits to their financial institutions. Digital information captured at the home or business is transmitted to the financial institution or its service provider for clearing and settlement. Financial institutions might also use RDCS in their branches and automated teller machines (ATMs) to facilitate deposit processing.

When properly managed, RDCS can reduce processing costs, support new and existing products of financial institutions and accelerate the availability of customers' funds. However, RDCS also introduces new risks and increases existing risks in processing deposits originated by an institution's commercial or retail customers, or by customers of other financial institutions domestically and abroad.

The guidance, “*Risk Management of Remote Deposit Capture*,” addresses the essential elements of RDCS risk management: identifying, assessing and mitigating risk, as well as measuring and monitoring residual risk exposure. The guidance also discusses the responsibilities of senior managers in overseeing the development, implementation and operation of RDCS in their financial institutions.

Risk Management and Controls for Remote Deposit Capture can be monitored in two ways, depending on the level of risk determined by the financial institution: I.T. Audit conducted by an independent/internal auditor or by completing the Risk Self-Assessment form in this document. The financial institution, in its sole discretion, must determine which method may be used by the Customer/Customer.

If you have any questions concerning the Self-Assessment, please contact the financial institution that provides you with Remote Deposit Capture service.

AUDIT WORK PROGRAM

RISK SELF-ASSESSMENT

DOCUMENTATION REQUEST

The following documents and reports are necessary to complete the Risk Self-Assessment. If you do not have a document or report, please indicate by writing "DNH (Do Not Have)" beside the item.

Legal Name: _____

FINANCIAL/BUSINESS INFORMATION

Structure of Ownership

___ Individual/Joint ___ Sole Proprietorship ___ Partnership ___ LLC ___ Corporation

___ Other (describe: _____)

Company Established: ___/___/_____ Employer/Tax ID Number: _____

Individual Social Security Number: _____

Type of Company or Employer:

_____

Date Incorporated/Filed DBA: _____ State of Incorporation: _____

Is Company required to register as a Money Service Business (MSB)? If yes, please provide copy of Money Service Business License Application.

OTHER DOCUMENTS PROVIDED OR ON FILE WITH FINANCIAL INSTITUTION

___ Assumed Name Certificate ___ Partnership Agreements ___ Other (describe: _____)

___ Guarantor Statement ___ Prior Year Tax Return ___ Financial Statements (year: _____)

___ Credit References ___ Credit Reports

MANAGEMENT REPORTING

1. Management Reports and Minutes that pertain to the presentation and approval of RDCS, Risk Management and Information Technology (IT) Audit of your company.
    a. Incident, Breach or ID Theft Report to Management if it occurred
    b. Actions taken since Breach or ID Theft to prevent future occurrence
2. How many fulltime employees (FTE) are employed by your company? _____

    (please include a current organization chart with functions)
3. What new systems were installed, or are planned for installation, since the last IT Audit?

    _____

OFFICES

1. Where are your offices located?

   City: _____State: _____ Country: _____

   City: _____State: _____ Country: _____

   City: _____State: _____ Country: _____

   City: _____State: _____ Country: _____

ESTIMATED DEPOSIT ACTIVITY

#	Account Title/Name	Account Number	Estimated Maximum Deposit Amount	Estimated Maximum Item Count	Estimated Deposit Frequency (daily, monthly, varied)
1					
2					
3					
4					

TECHNOLOGY POLICIES, PROCEDURES & ASSESSMENTS

1. Policies and Procedures
   a. Security Risk Assessment
   b. Destruction Policy for captured checks, media and obsolete electronic equipment
   c. Information Technology (I.T.) Policy for security and use of network, email and passwords
   d. Computer Patch Management Policy
   e. Information Technology (IT) Audit Policy
   f. Privacy Policy
   g. Employee New Hire and Termination Policy
   h. Vendor Oversight Policy
2. Risk Assessment completed and published prior to RDCS conversion
3. Agreement between Financial Institution and Customer
4. Exposure limit assigned to Customer
5. Service Level Agreement (SLA) between Customer and network maintenance vendor
6. Description of training program for Remote Deposit Capture System
7. Image Quality Assurance (IQA) procedures for testing images after capture
8. Description or copy of balancing procedures
9. Current Business Continuity Plan (BCP)

    a. Report of BCP test

10. Retention schedules for captured checks
11. Date you started using Remote Deposit Capture System?_____
12. What is current sales in (USD) of the Company? _____
13. Have you had server capacity issues during the past year?

    If yes, please explain: _____

14. Have you had any security breaches during the past year?

    If yes, please explain: _____

15. Who is the Electronic Security Officer? _____
16. Name and location of:
    a. Technology Provider _____
        i. In-house _____ (Y/N)
17. Is network maintenance performed:
    a. In-house staff _____ (Y/N)
    b. Outsourced - Company Name: _____

RISK SELF-ASSESSMENT WORK PROGRAM

AUDIT PREPARATION	Performed By:	Workpaper Ref:
1. Review the minutes from Management meetings over the past year, noting reports of information systems activities and approval/updates of Remote Deposit Capture Risk Assessment and Policies and Procedures.		
2. Review prior audit reports (internal and external) and determine if all noted violations or weaknesses were corrected.		
3. Determine the scope of the Assessment, based on the size, complexity and evaluation of internal controls and the work performed by the previous examiners.		
MANAGEMENT AWARENESS OF REQUIREMENTS	**Performed By:**	**Workpaper Ref:**
4. Determine if the Management has adopted a written audit program that includes: a. A system of internal controls to ensure ongoing compliance. b. Independent testing for compliance conducted by either independent and qualified Company employee or an outside audit firm. c. Initial and ongoing risk management program, which includes publishing a "Report of Findings" to Management. d. Designation of a qualified individual(s) responsible for coordinating and monitoring day-to-day compliance.		
5. Was the Management apprised of Check 21 Law and other applicable regulations and changes during the past year?		
6. Has any breach or internal fraud occurred during the past year? a. If yes, was a report filed with the sponsoring financial institution and appropriate law enforcement agency?		
LEGAL & COMPLIANCE	**Performed By:**	**Workpaper Ref:**
7. Was Company provided with adequate explanation of Legal Warranties pertaining to Remote Deposit Capture: a. Duplicate items presentment? b. Image quality? c. Items drawn on U.S. financial institutions only? d. Use of check carriers is prohibited by Federal Reserve Bank?		

8. Was Duty to Discover and Report Unauthorized Transactions adequately explained to Company?		
PERFORMANCE STANDARDS	**Performed By:**	**Workpaper Ref:**
9. Is Service Level Agreement established? a. If yes, is service being provided in accordance with Agreement?		
CUSTOMER AWARENESS AND ISSUES	**Performed By:**	**Workpaper Ref:**
10. Is Customer aware of any fraud that resulted in legal action?		
11. Did attorney review all RDCS related agreements?		
DISCLOSURES	**Performed By:**	**Workpaper Ref:**
12. Has Company provided compliance disclosures for any technology used that requires customer notification or opt-out procedures?		
BUSINESS REQUIREMENTS	**Performed By:**	**Workpaper Ref:**
13. Was business plan developed and presented to Management?		
14. Does Exposure Limit meet the needs of the Customer?		
15. Is there a contingency plan for RDCS in the event of a disaster?		
16. Are Return Items (NSF) handled in a timely manner?		
17. Is Deposit Deadline appropriate for Company?		
SYSTEM ACQUISITION	**Performed By:**	**Workpaper Ref:**
18. Was integration with other systems planned and documented for RDCS? a. Return item and exception item processing.		
19. Are reports from RDCS system adequate?		
20. Was a system Service Level Agreement (SLA) established before the system was placed into production?		
CUSTOMER SUPPORT	**Performed By:**	**Workpaper Ref:**
21. Are Customer Support requirements documented and approved?		
22. Is there a system for tracking and resolving customer issues?		
23. Are Error Resolution procedures documented and understood?		

PERSONNEL REQUIREMENTS	Performed By:	Workpaper Ref:
24. Has a formal training program been developed and implemented for the staff? a. If yes, what is frequency of training?		
25. Review the training program to determine if the following elements are adequately addressed: a. The appropriateness of the scope and frequency of training. b. Coverage of Policies and Procedures. c. Legal requirements for preventing Identity Theft and Fraud. d. Coverage of new rules and requirements.		
26. Are Human Resources' policies and procedures maintained that include background checks on personnel that will operate or have significant access to information collected through RDCS?		
27. Are separation of duties followed, where possible?		
IMAGE QUALITY	**Performed By:**	**Workpaper Ref:**
28. Are Image Quality Assurance (IQA) modules operational and used?		
29. Are IQA standards validated?		
BALANCING AND CONTROLS	**Performed By:**	**Workpaper Ref:**
30. Are balancing controls and procedures provided by the financial institution defined and used by Operations' staff?		
31. Are balances and transactions reviewed each day for accuracy of previous day's activities?		
INSURANCE	**Performed By:**	**Workpaper Ref:**
32. Has insurance coverage of pertinent risks and liabilities been reviewed since implementation of Remote Deposit Capture and is it a scheduled annual review? a. Was report of findings issued to Management?		
SYSTEM MAINTENANCE AND ENHANCEMENTS	**Performed By:**	**Workpaper Ref:**
33. Is network maintained in accordance with the I.T. Patch Management Policy?		

RISK ASSESSMENT	Performed By:	Workpaper Ref:
34. Was Risk Self-Assessment conducted during past year? a. If yes, was Report of Findings published to Management?		
35. Does annual Risk Assessment include RDCS?		
36. Determine if management has established procedures to review transaction activity through electronic banking products for possible money laundering and suspicious activity.		
37. Determine if the Management and senior management have developed policies and procedures that comply with OFAC laws and regulations, including: a. Maintaining a list of prohibited countries, entities, and individuals. b. Monitoring transactions for possible prohibited activity, including transactions through non-bank financial institutions, if applicable.		
38. Was Vulnerability Assessment conducted during the past year, which included: a. Internal and External Penetration Test? b. Review of Security Patch Management? c. Verification that Virus Detection updates are applied in a timely manner? d. Testing workstations to ensure layered security?		
DISASTER RECOVERY	**Performed By:**	**Workpaper Ref:**
39. Has RDCS been added to disaster recovery workplans for testing?		
40. Has RDCS disaster recovery/business continuity plan been tested? a. If yes, was Report published to Management?		
RECORD RETENTION AND DESTRUCTION	**Performed By:**	**Workpaper Ref:**
41. Are checks kept in a safe environment to avoid theft?		
42. Is check container marked with Capture Date and Destroy Date?		
43. Are Item Processing records retained for five years and retrievable?		

COMPLETING THE ASSESSMENT	Performed By:	Workpaper Ref:
44. Summarize findings and publish Risk Assessment Report for management and financial institution.		
45. Review the exceptions documented in the Assessment with management and financial institution.		

Comments:

_____

_____

_____

_____

_____