

	A	B	D
3	<b>Remote Deposit Capture Examination Procedures</b>		
4	<b>Objective: Evaluate and document the Remote Deposit Capture activities</b>		
5		<b>Yes/No</b>	<b>Comments</b>
6	<b>I. General - Service Delivery Environment</b>		
7	1. Identify the parties involved, their responsibilities, and their transaction volumes in the Remote Deposit Capture (RDC) function.		
8	2. Review the credit union network topology to determine the infrastructure involved with RDC.		
9	3. Review the credit union's data flow or process flow diagram to understand the RDC function, relationship with third party processor (if applicable), and relationship with RDC client.		
10	<b>II. Management – Strategic Planning/Risk Assessment/Policies and Procedures</b>		<b>Comments</b>
11	<b>a. Strategic Planning</b>		
12	1. Has the Board of Directors or Senior Management developed a formal strategic plan for the implementation of RDC?		
13	<b>b. Risk Assessment</b>		
14	2. Has management completed a risk assessment related to remote deposit capture? The risk assessment should encompass factors such as: • Scope of product • Type of member • Credit union position in payment process (BOFD (Bank of First Deposit) vs. non-BOFD) • Anticipated volume of RDC transaction • Member role/responsibility in RDC process • Member ability to download/retain NPI (non-public information) • Credit Union-approved vendors and equipment • System: image-only or can member create ACH		
15	3. Is the RDC risk assessment reviewed on an annual basis and updated as technology, market, member base, industry, or processes change?		
16	4. Does the risk assessment process include input from other functions at the credit union, such as Credit, IT, Deposit Operations, Internal Audit, and Legal, etc.?		
17	5. Does the credit union plan to/currently provide member service or support to the RDC clients? If yes, did they address the need for additional staff?		

	A	B	D
18	<b>c. Policies and Procedures</b>		
19	6. Does the credit union have policies and procedures for RDC and have they been reviewed by the Board? e.g. Do they define the function, responsibilities, operational controls, vendor management, customer due diligence, and reporting functions, etc.?		
20	<b>III. Due Diligence - Vendor / Member / Application Specifications</b>	<b>Yes/No</b>	<b>Comments</b>
21	<b>a. Due Diligence - Member</b>		
22	1. Does the credit union have a due diligence process to review and rate potential candidates for the RDC delivery system? <ul style="list-style-type: none"> <li>• How does the credit union risk rate existing members?</li> <li>• How does the credit union qualify potential members?</li> <li>• Does the credit union review: member application, financial analysis, years in business (for commercial members), loan/deposit history, credit score, business practices, sufficiency of staff, compliance with PCI standards (Payment Card Industry Standards )?</li> <li>• Does the credit union review Visa/MasterCard terminated merchant file or Chex Systems report?</li> <li>• Does the credit union have procedures that address the performance of CIP (customer identification program) as explained in the BSA manual?</li> </ul>		
23	2. Has the credit union management evaluated the RDC client's information security infrastructure?		
24	3. Is there ongoing or periodic monitoring of the member?		
25	4. Has credit union management assessed the need and/or availability of RDC insurance products?		
26	<b>b. Applications Specifications</b>		
27	5. Did management consider the following features or functionality when making their vendor or application decision? <ul style="list-style-type: none"> <li>• Duplicate item detection</li> <li>• Scanner options (simplex/duplex (scan both sides of double-sided originals), MICR (Magnetic Ink Character Recognition)/OCR (Optical Character Recognition), franking/spraying, CAR (Courtesy Amount Recognition) /LAR (Legal Amount Recognition), etc.)</li> <li>• Interoperability with existing systems and/or ancillary applications (e.g. QuickBooks)</li> <li>• MIS (Management Information System) and reporting (audit logs, activity reports)</li> <li>• Image Quality</li> <li>• Ability to change MICR, account number, and amount</li> <li>• Least Cost Routing functionality (conversion into different payment stream)</li> </ul>		

	A	B	D
28	<b>IV. Legal &amp; Compliance / Contracts &amp; Agreements / Internal Audit</b>	<b>Yes/No</b>	<b>Comments</b>
29	<b>a. Legal &amp; Compliance</b>		
30	1. Is legal counsel involved in drafting the special merchant agreement?		
31	<b>b. Contracts &amp; Agreements</b>		
32	2. Does the contract or agreement between the credit union and the merchant client contain the following:		
33	2.a <ul style="list-style-type: none"> <li>• Funds availability and reject/return guidelines</li> <li>• Liability transference</li> <li>• Warranty and indemnification provisions</li> <li>• System maintenance and administration guidelines (change control &amp; logical access administration)</li> <li>• Dispute resolution/contract termination provisions</li> <li>• Information security guidelines and procedures</li> <li>• Credit union's right to audit provision, request self-assessment</li> <li>• Security incident reporting</li> <li>• Member service support</li> </ul>		
34	2.b <ul style="list-style-type: none"> <li>• Responsibility for network connectivity</li> <li>• Establish controls such as deposit limits, overdraft limits, and payment on uncollected funds</li> <li>• Physical check retention timeframes and secure storage at RDC client</li> <li>• Business Continuity Plan/Disaster Recovery Plan provision (advise member of responsibility to plan for service interruptions)</li> <li>• Scalability</li> <li>• Limiting item capture to one account</li> <li>• Retention timeframes of check images (at the credit union or the technology service provider)</li> </ul>		
35	3. Does the credit union have service level agreements (SLAs) that would provide baselines for services provided? <ul style="list-style-type: none"> <li>• Availability and processing timeframes (system uptime, check submission timeframes, funds availability/return items, etc.)</li> <li>• Report availability timeframes (when reports are available for client review)</li> <li>• Exception volume limits (rejects, duplicate items, etc.)</li> <li>• BCP responsibility, business recovery timeframes, and periodic tests results</li> <li>• Help desk support (availability, type, channel)</li> </ul>		
36	<b>c. Internal Audit</b>		
37	4. Does Internal Audit review RDC activities and compliance with the RDC policy/procedures?		
38	5. Does the credit union have a process for auditing their RDC customers? <ul style="list-style-type: none"> <li>• Does the credit union perform any on-site reviews at the merchants?</li> <li>• Does the credit union review self-assessments from the RDC merchants/members?</li> <li>• Do they receive/review penetration tests, audit reports, vulnerability assessments, etc.?</li> </ul>		

	A	B	D
39	<b>V. Operational (Implementation)</b>	<b>Yes/No</b>	<b>Comments</b>
40	<b>a. Access Controls (Physical/Logical)</b>		
41	1. Has credit union management ensured that there are appropriate physical security controls at the RDC client location? (e.g. secure building - locks, alarm system, secure storage of checks - safe, shredder for check destruction)		
42	2. Has credit union management ensured that there are appropriate logical security controls at the RDC client location? (e.g. encrypted data transmission, multi-factor authentication, access level controls, password security parameters, etc.)		
43	3. Is any data ((check images or documents) that contains Non-Public Customer Information(NPCI)) stored locally on the RDC client PCs? If yes, is that data encrypted? This includes cache RAM and other storage devices.		
44	<b>b. Separation of Duties</b>		
45	4. Has management established appropriate separation of duties of the system administration and security monitoring functions? (e.g. Does the individual assign users or rights also review the activity reports?)		
46	5. Does the credit union ensure that RDC clients implement appropriate separation of duties controls over the remote capture and transmission process?		
47	6. If the credit union performs any data entry functions (e.g. adjusting dollar amounts), is there an independent review or reconciliation?		
48	<b>c. Audit/Monitoring</b>		
49	7. Does management routinely review logical and physical access privileges and audit trails/logs?		
50	8. Does the RDC client conduct self-audits or self-assessments of processes to ensure compliance to contracts and service level agreements?		
51	9. Does credit union management routinely review: <ul style="list-style-type: none"> <li>• Double Presentment Report (to detect duplicate batches prior to submission)</li> <li>• Daily Batch Totals Report</li> <li>• Velocity Exception Report (to detect merchant spikes in volume or exceeding approved dollar limits)</li> <li>• Large Item Report (exception report to detect transactions are outside of normal parameters)</li> <li>• Client Activity Report (detailed log of activity by merchant, including batch delivery date, time, value, receipt acknowledgement, and merchant operator ID)</li> </ul>		
52	10. Does management recommend/ensure that RDC clients review the following reports: <ul style="list-style-type: none"> <li>• Pending Batch Report (items queued for processing for reasonableness and timeliness reviews)</li> <li>• Batch Total Report (allows the merchant to reconcile processed RDC work to the batch prepped for submission to the credit union)</li> <li>• Return Item Report (alerts management to operational deficiencies e.g. poor image quality)</li> <li>• Double Presentment Report (to detect duplicate batches prior to submissions)</li> <li>• Financial Institution Reports (report would provide list of received imaged items)</li> </ul>		

	A	B	D
53	11. Does the credit union monitor activity versus pre-set limits to ensure continued appropriateness?		

	A	B	D
54	<b>d. Training</b>		
55	12. Has credit union management established a training program to ensure that all involved entities are appropriately trained?		
56	13. Has management provided incident response training to the merchant/consumer to ensure they are aware of the procedures and contact information?		
57	14. Does the credit union provide training to the credit union employees on the new delivery system and methods of responding to merchant/consumer questions?		
58	15. Does the credit union provide training to the merchant/consumer clients to ensure they are appropriately educated on the use and risks of the system? The training should include: <ul style="list-style-type: none"> <li>• demonstrating the application and scanner,</li> <li>• how the scanner works and problems with it (e.g. bad MICR, rejects),</li> <li>• manual data entry, and</li> <li>• forced balancing, etc.</li> </ul>		
59	16. Does the credit union provide the merchant/consumer clients with a procedural or instructional document and a user guide for the application/scanner?		
60	<b>e. Change Management</b>		
61	17. Has the credit union updated their change management program to address the procedures involved in the RDC function?		
62	18. If the credit union maintains the application in-house, does it ensure that all relevant operating system and application patches are up-to-date?		
63	19. Has credit union management ensured that RDC clients understand the need to implement an effective change management program to maintain updated and patched operating system, RDC application, and anti-virus, etc.?		
64	<b>f. Records Management</b>		
65	20. Does the credit union include physical check retention timeframes in the contract and is the RDC client complying with the contract stipulation?		
66	21. Does the credit union include secure storage guidelines in the contract and is the RDC client complying with the contract guidelines?		
67	22. Does the credit union include appropriate check destruction practices in the contract and is the RDC client complying with them?		
68	<b>g. Business Continuity Planning</b>		
69	23. Has the credit union's business continuity plan been updated to address: <ul style="list-style-type: none"> <li>• The credit union's relationship with the RDC service provider and BCP assurance</li> <li>• The credit union's relationship with the RDC client</li> </ul>		

	A	B	D
70	<b>VI. Fraud</b>	<b>Yes/No</b>	<b>Comments</b>
71	1. Is credit union management aware of fraud associated with the implementation of RDC?		
72	2. How the credit union monitor the fraud or otherwise attempt to mitigate risks? (e.g. duplicate check detection, establishing deposit limits, safeguarding checks, etc.)?		
73	3. For what duration does the credit union or the TSP retain check images for the purpose of duplicate check detection?		
74	<b>Overall Questionnaire Comments:</b>		
75			

**Cell:** A7

**Comment:** Determine complexity of the function and technology.

**Cell:** A8

**Comment:** Determine if the credit union has considered appropriate security controls over IT.

**Cell:** A9

**Comment:** Determine if management understands the work flow.

**Cell:** A12

**Comment:** A written strategy may not be warranted depending on the size and complexity of the credit union, or the scale of implementation. However, at a minimum, the board or senior management should be able to articulate the organization's strategy. If there is no written strategic plan, interview relevant management and board members to obtain the information.

In addition, management should determine if the product/delivery system is the right fit.

**Cell:** A14

**Comment:** Development of the risk assessment will assist the credit union to identify possible risks related to RDC and to establish controls that mitigate those risks.

**Cell:** A15

**Comment:** Determine if management is adjusting the risk assessment annually according to regulation.

**Cell:** A16

**Comment:** Involve all relevant departments to ensure all RDC risks are identified.

**Cell:** A17

**Comment:** This would demonstrate that management prepared appropriately for higher volume of calls and that staff is sufficiently trained.

**Cell:** A19

**Comment:** Policies and procedures define the function, responsibilities, and controls of RDC.

**Cell:** A22

**Comment:** Given the member's involvement in the check processing, client due diligence will ensure appropriate clients and potentially minimize fraud. If the credit union does not pre-qualify and "know" their members, they will not know the risks associated with providing them this system.

Note that the Chex Systems, Inc network is comprised of member Financial Institutions that regularly contribute information on mishandled checking and savings accounts to a central location.

Chex Systems shares this information among member institutions to help them assess the risk of opening new accounts.

**Cell:** A23

**Comment:** This would mitigate potential security vulnerabilities related to RDC.

**Cell:** A24

**Comment:** This would identify changes in RDC client behavior, either positive or negative.

**Cell:** A25

**Comment:** the CUMIS Credit Union Bond does cover RDC. Examiners should inquire if the credit union has obtained a legal opinion or insurance company assurance of coverage (e.g., a settled claim).

**Cell:** A27

**Comment:** The risk assessment results should drive the functionality of the system. Based on the findings of the risk assessment, the application features and functionality should match the defined specifications .

This information is required to understand the RDC system's functionality. If the credit union has multiple systems, examiners should obtain this information for each system implemented.

QuickBooks is an accounting software for small business financial management and bookkeeping.

**Cell:** A30

**Comment:** With legal counsel advice, the credit union's interests will be protected.

**Cell:** A32

**Comment:** Contracts define each party's responsibility in the event of a dispute. Credit union management must ensure that they use the contract/agreement to appropriately transfer liability to the merchant/member.

**Cell:** A35

**Comment:** Service Level Agreements should define the expectations of each party.

**Cell:** A37

**Comment:** Independent review is required by regulation for information security.

**Cell:** A38

**Comment:** Prudent practices dictate that credit union management have some method of review to ensure their RDC clients are adhering to contract stipulations.

**Cell:** A41

**Comment:** Clients are responsible for the protection of Non-Public Information.

**Cell:** A42

**Comment:** Clients are responsible for the protection of Non-Public Information in transmission and storage.

**Cell:** A43

**Comment:** Clients are responsible for the protection of Non-Public Information in transmission and storage.

**Cell:** A45

**Comment:** To minimize abuse or fraud within the system, prudent practice dictates the need for separation of duties.

**Cell:** A49

**Comment:** Routine log monitoring will detect and minimize fraud.

**Cell:** A50

**Comment:** Ensure adherence to contract and agreements.

**Cell:** A51

**Comment:** Credit union management must be aware of the activities of their RDC clients. Routine report monitoring will detect and minimize fraud.

**Cell:** A52

**Comment:** Routine report monitoring at the RDC client will allow for effective business operating processes and potentially identify fraud.

**Cell:** A53

**Comment:** Spikes in volume could be indicative of duplicate processing or simply of increased business.

**Cell:** A55

**Comment:** A well designed and formalized training program is an effective mechanism for educating employees and RDC clients.

**Cell:** A56

**Comment:** Incident response training and contact information will ensure merchants are aware of their responsibilities to report incidents.

**Cell:** A57

**Comment:** This will ensure employees are aware of their responsibilities on the system and ability to respond to customers.

**Cell:** A58

**Comment:** Training will reduce errors, reduce member calls, and increase efficiency.

**Cell:** A59

**Comment:** A procedural/instructional document will provide some administrative information and security best practices to the RDC clients. A user guide will provide documentation for the application and scanner.

**Cell:** A61

**Comment:** Effective change management programs reduce the risk of unauthorized changes or compromised systems.

**Cell:** A62

**Comment:** Effective change management programs reduce the risk of unauthorized changes or compromised systems.

**Cell:** A63

**Comment:** Effective change management programs reduce the risk of unauthorized changes or compromised systems.

**Cell:** A65

**Comment:** Adhere to the contract stipulations on the retention timeframes to ensure they do not destroy a check before it has posted and do not retain a check for an extended timeframe.

**Cell:** A66

**Comment:** Checks must be appropriately destroyed (e.g. shredded) to ensure they are not inappropriately used.

**Cell:** A67

**Comment:** Checks must be appropriately destroyed (e.g. shredded) to ensure they are not inappropriately used.

**Cell:** A69

**Comment:** To ensure that the RDC activity is incorporated in the BCP and that all involved entities are aware of their responsibilities during a disaster.

**Cell:** A71

**Comment:** FRAUD = BAD! Management should be aware that RDC presents new fraud exposures that must be controlled.

**Cell:** A72

**Comment:** Without monitoring mechanisms, it could take days or weeks to determine that fraudulent activity occurred.

**Cell:** A73

**Comment:** Several TSPs offer duplicate check detection and retain check images for up to 180 days. This should provide an adequate window of review to minimize the risk of an RDC client attempting to redeposit checks.