

FFIEC Guidance on Risk Management of Remote Deposit Capture Digest of Key Elements

Full text of FFIEC Guidance: <http://files.ots.treas.gov/482031.pdf>

The following document outlines the salient points of the FFIEC Guidance on Risk Management of Remote Deposit Capture. Please click on the link above for the full text of the guidance for additional information.

Overview

- Key areas of risk with RDC for FIs offering it:

- <FRAUD & CRIMINAL MISUSE>
- <REGULATORY & COMPLIANCE>
- <OPERATIONAL & LEGAL>
- <CREDIT>
- <COMPETITIVE>
- <REPUTATIONAL>

In other words, virtually all areas of risk are encompassed.

- Definition/description: “Remote Deposit Capture (RDC), a deposit transaction delivery system, allows a financial institution to receive digital information from deposit documents captured at remote locations. These locations may be the financial institution’s branches, ATMs, domestic and foreign correspondents, or locations owned or controlled by commercial or retail customers of the financial institution.” (The Guidance)
- RDC is a new *delivery system*, not just a new product or service.
- The promise and the challenge: “RDC can decrease processing costs, support new and existing banking products, and improve customers’ access to their deposits; however, it introduces additional risks to those typically inherent in traditional deposit delivery systems.” (The Guidance)
- The principles of RDC risk management generalize; e.g., to mobile banking and ACH check conversion (as well as internal deployment of RDC at branches and ATMs). What’s specified here can be utilized elsewhere.

Risk Management Oversight

- Involve the right areas of your *organization*:
 - Board & management oversight (as appropriate to the size of the organization)
 - Information technology
 - Deposit operations (& float management)
 - Treasury/cash management sales
 - Business continuity
 - Information security
 - Audit
 - Compliance
 - Accounting
 - Legal

- Key components of an RDC *risk management policy*:
 - level of risk tolerance defined
 - specification of procedures and controls
 - risk transfer mechanisms, as appropriate (e.g., agreements)
 - well-designed contracts
 - risk measurement
 - risk monitoring
 - standards; reporting against standards
 - periodic risk assessments
 - velocity metrics (# of files; \$; returns; etc.)
 - reporting: point in time vs trending; customer, groupings, overall

- Insurance coverage

Customers <OPERATIONAL; CREDIT; FRAUD>

- Know Your Customer (KYC):
 - Exercise stringent customer selectivity for RDC (their business activities; their risk management practices; geographic location; *their* customer base).
 - Identify need for customer training.

- Customer *agreements*:
 - Identify roles and responsibilities.
 - Allocate risks appropriately (warranties; indemnification).
 - Identify types of items that can be deposited.

 - Specify processes and procedures that must be followed
 - Specify management of checks (processing, transmission, storage, destruction) at customer location.
 - Identify explicit controls that need to be in place.
 - Establish mandated internal controls.
 - Set performance standards.
 - Spell out consequences of non-performance.
 - Define image quality requirements.

 - Define funds availability.
 - Define return timeframes.

 - Establish customer audit requirements.
 - Reserve right to customer site visits and suitability reviews:
 - ✓ -operational controls
 - ✓ -risk management practices
 - ✓ -staffing
 - ✓ -need for training and support
 - ✓ -IT infrastructure

 - Reserve right to provision of documents to resolve exceptions.
 - Set terms of dispute resolution.
 - Identify governing law.
 - Include termination clauses.

- Establish authentication measures required at time of processing.

Vendors <OPERATIONAL>

- Vendor agreements
- Project implementation
- Change control for hardware and software (coordinated with customer sites)

Additional operational considerations <OPERATIONAL/LEGAL; FRAUD;
REGULATORY/COMPLIANCE>

- Separation of duties
- Agreements with other FI exchange partners
- Adequate, documented procedures
- Adequate, ongoing training of staff
- Maintenance of equipment
- Least Cost Routing involves both ACH & Check Collection Systems. Be aware of the increased complexities (funds availability; return timeframes; differing rules and regulations; etc.)
 - Using ACH makes the customer an ACH originator; be sure to have an ACH originator agreement in place.
- Take account of added complexities if foreign branches or foreign money service businesses are involved with your RDC offering.
- Need physical and logical access controls over:
 - RDC systems
 - original deposit items (at customer site)
 - electronic files
 - nonpublic personal information (capture; transmission; storage; destruction)
- Transmission security (authentication; encryption)
- Risks inherent in check processing can be exacerbated in an RDC/image environment:
 - Check alteration (including MICR line)
 - Forged or missing endorsements
 - Lost security features (e.g., lowered ability to detect check washing)
 - Counterfeiting
 - Duplicate presentment (items; files)
 - Identity theft (e.g., by customer employees)
- Deposit authentication processes (see under Customers section above)

References cited in the Guidance

- Operational and fraud risk:
 - ✓ *FFIEC IT Examination Handbook*
(URL: <http://www.ffiec.gov/ffiecinfobase/index.html>)
 - *Operations booklet*
 - *Audit booklet*
 - *Management booklet*
 - *Business Continuity Planning booklet*
 - *Information Security booklet*
 - *Outsourcing Technology Services booklet*
 - ✓ *OCC 2006-35: Guidance on Authentication in an Internet Banking Environment*
 - ✓ *Interagency Guidelines Establishing Information Security Standards*

- Clearing and settlement risk:
 - ✓ *Reg CC*
 - ✓ *Reg J*
 - ✓ *Check 21 Act*
(URL: <http://www.ffiec.gov/exam/check21>)
 - ✓ *Applicable state laws, clearinghouse rules, or other agreements*

- Regulatory risk (terrorism & anti-money laundering):
 - ✓ *FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual* (URL: http://www.ffiec.gov/bsa_aml_infobase/default.html)
 - ✓ *USA PATRIOT Act*
 - ✓ *OFAC requirements*

The following items are likely to have additional attention by regulators as a result of the FFIEC Guidance on Risk Management of Remote Deposit Capture.

KEY EXAMINATION FLAGS

- Lack of oversight
- Lack of customer due diligence
- Inadequate limits (which should be logical and reasonable)
- Inadequate approval process (e.g., separation of duties)
- Lack of monitoring
- Lack of reporting

ITEMS EXAMINERS WILL LIKELY ADDRESS

Item	General	Customer-oriented	Operationally-oriented	Control-oriented	Vendor-oriented
Strategic plan	X				
FI's risk assessment	X			X	
Board/management oversight	X				
Volumes; number of customers		X	X		
Geography of customer base		X			
Customer selection process		X			
Customer due diligence; credit analysis		X		X	
Customer distribution by risk rating		X			
Training		X	X		
Records management (retention; destruction/shredding of checks)		X	X	X	
Policies & procedures			X		
Monitoring		X		X	
Staff			X		
Data flows			X	X	
Change management		X		X	X
Internal controls (separation of duties)				X	

Item	General	Customer-oriented	Operationally-oriented	Control-oriented	Vendor-oriented
System capabilities (e.g., limit parameters)				X	
Physical & logical security				X	
Insurance coverage	X				
Safeguards against check alteration, counterfeits, etc.				X	
Vendor relationships					X
Contracts & agreements		X			X