Remote Deposit Capture Annual Review Checklist

Company Name:	

1.	Describe the safeguards used by your organization to ensure the confidentiality & integrity of User ID's and Passwords used to access Remote Deposit Capture (RDC).	
2.	Do you enforce complex passwords? How are they protected?	
3.	Are user passwords saved on the RDC workstation?	☐ Yes ☐ No
4.	Is the workstation designated for RDC only?	☐ Yes ☐ No
5.	What operating system is installed on the RDC workstation?	
6.	How long do you retain scanned checks before destroying them? ***You are required to destroy scanned checks no earlier than 30 days and no later than 45 days***	
7.	Is the line printed on the check by the scanner legible? Does it print on the front or the back?	☐ Yes ☐ No ◯ Front ◯ Back
8.	Where are your checks stored after being scanned and before being destroyed?	
9.	Is the RDC workstation segmented (e.g., Virtual Local Area Network or VLAN) and isolated from other devices?	

10.	**Is a vulnerability management system used to scan for the operation system and application/software vulnerabilities and configurations? How often does your organization run scans?**	
11.	**How often are patches/updates applied? How are critical vulnerabilities prioritized?**	
12.	**Does Patch Management (i.e., installation of updates) apply to the operation system and ALL applications installed on the RDC workstation?**	☐ Yes ☐ No
13.	**What type of endpoint protection is used to defend against malicious software (malware)? Is it Next Generation (NextGen)?**	
14.	**Does your organization use Endpoint Detection and Response (EDR)?**	☐ Yes ☐ No
15.	**Did your organization establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack?**	☐ Yes ☐ No
16.	**Is the RDC workstation physically secured? How?**	
17.	**Which Internet browser does your organization use to access the online Remote Deposit Capture (RDC)? Are updates applied promptly based on a pre-approved Service Level Agreement (SLA)?**	
18.	**Does your organization use Internet Content filtering and Cloud Cybersecurity?**	☐ Yes ☐ No
19.	**Does your organization utilize phishing campaigns to test awareness and provide training to the user community?**	☐ Yes ☐ No

COMPANY'S REPRESENTATIVE PERFORMING DEPOSITS:

Acknowledged By: _____ Date: _____

Name and Title

Signature: _____

COMPANY'S INFORMATION TECHNOLOGY REPRESENTATIVE:

Acknowledged By: _____ Date: _____

Name and Title

Signature: _____

COMPANY'S AUTHORIZED SIGNER (*PER CORPORATE RESOLUTION*):

Acknowledged By: _____ Date: _____

Name and Title

Signature: _____

BANK'S REPRESENTATIVES *(for bank purposes only)*:

Electronic Banking: _____ Date: _____

Name and Title

Signature: _____

IT (Info Sec): _____ Date: _____

Name and Title

Signature: _____