



Internal Controls – Self Assessment

Physical Location: _____

Date(s) _____

A.	Cash Handling Procedures	OK or N/A	We Need Help
	<ul style="list-style-type: none"> When were staff last trained to do a “cash flow” analysis? _____ Who did the training? _____ 		
	<ul style="list-style-type: none"> When was the last “surprise” cash count and what was included? _____ Why was it considered a surprise? _____ 		
	<ul style="list-style-type: none"> What’s the most currency kept at any teller station during the last 18 months? _____ Was it split between two locked containers at the counter? _____ 		
	<ul style="list-style-type: none"> Who verifies currency received from the bank? _____ 		
	<ul style="list-style-type: none"> How many drawers (locked) are used at each teller station? _____ What per cent of front line teller currency is kept in the primary drawer? _____ 		
	<ul style="list-style-type: none"> How are tellers disciplined when they leave their station and don’t lock their drawer/tray? _____ 		
	<ul style="list-style-type: none"> How is access to the central change fund/vault cash controlled? _____ If a shortage occurs, how will you determine who’s responsible? _____ 		
	<ul style="list-style-type: none"> How many tellers work out of the same traveler check inventory? _____ If a shortage occurs, how will you determine who’s responsible? _____ 		
	<ul style="list-style-type: none"> How are spare keys stored and safeguarded against unauthorized use? _____ 		
	<ul style="list-style-type: none"> How many tellers share a teller drawer or tray? _____ Why is this allowed and how will you determine who’s responsible for a loss from a shared drawer/tray? _____ 		
	<ul style="list-style-type: none"> What is the burglary resistant rating on the safe/vault in which currency and traveler checks are stored during non-business hours? _____ 		
	<ul style="list-style-type: none"> How many employees have <u>all</u> the keys, codes and combinations needed to void all security systems? _____ How are these employees protected against extortion? _____ 		

<p>_____</p> <p>_____</p>		
<ul style="list-style-type: none"> • How are combinations protected when they're written down? _____ 		
<ul style="list-style-type: none"> • When were employees last trained in a "clean office" policy focused on safeguarding confidential information? _____ • How do you safeguard against "dumpsite" diving? _____ 		
<ul style="list-style-type: none"> • What's your policy regarding employees cashing their own checks or posting to their own accounts? _____ • How do you monitor and enforce this policy? _____ 		
<ul style="list-style-type: none"> • When are checks restrictively endorsed? _____ 		
<ul style="list-style-type: none"> • Are supervisory override controls used? _____ • How often is the supervisory override printout reviewed and who reviews it? _____ 		
<ul style="list-style-type: none"> • How is access to computer terminals controlled? _____ 		
<ul style="list-style-type: none"> • When was the last time your expense policy was updated? _____ • Who approves expense reimbursements? _____ • Prior to payment, are corporate expenses, including credit card charges, reviewed and approved by the next higher level of supervision? _____ • Does the individual who approves expense accounts also have general ledger posting authority? _____ 		
<ul style="list-style-type: none"> • Who reviews suspense account activity? _____ • Do they have posting authority? _____ 		
<ul style="list-style-type: none"> • Who reviews the overdraft printout? _____ • Do they have posting authority? _____ 		
<ul style="list-style-type: none"> • How are dormant and inactive accounts safeguarded against unauthorized use? _____ 		
<ul style="list-style-type: none"> • How are signature machines and signature plates protected during business and non-business hours? _____ 		
<ul style="list-style-type: none"> • How are blank checks stored and protected against unauthorized use? _____ 		
<ul style="list-style-type: none"> • When were the checking accounts reconciled by someone who was not authorized to sign checks? _____ 	OK or N/A	We Need Help
<ul style="list-style-type: none"> • What dual controls are used to verify mail deposits? _____ 		

<ul style="list-style-type: none"> • What dual controls are used to verify night deposits? _____ _____ • Is a log/record documented for each opening of the night depository? _____ 		
<ul style="list-style-type: none"> • When was your written overdraft policy updated? _____ 		
<ul style="list-style-type: none"> • When was your availability policy updated? _____ 		
<ul style="list-style-type: none"> • When were employees last asked to sign and date the credit union "fraud" policy? _____ 		
<ul style="list-style-type: none"> • How do you verify an employ can be bonded? _____ _____ 		
<ul style="list-style-type: none"> • When were tellers trained in forgery detection techniques? _____ • What was taught? _____ _____ 		
<ul style="list-style-type: none"> • When were tellers trained to recognize a forged ID _____ What was included in their training? _____ 		
<ul style="list-style-type: none"> • When were employees trained to detect kiting? _____ What were they taught? _____ _____ 		
<ul style="list-style-type: none"> • Who monitors forgery and fraudulent deposit losses? _____ _____ 		
<ul style="list-style-type: none"> • Who monitors and files bond claims? _____ _____ 		

Use this space for notes during the self assessment. Report your finding to the Supervisory Committee and your Internal Auditor. All indicators of fraud should be reported immediately to your bonding company. Your bond is a contract of good faith. Your knowledge of fraud or dishonesty must be reported or your coverage on the suspect might terminate the moment you discovered the dishonest act.