Fraud Evaluation Tool

COMMERCIAL BANKING &
TREASURY MANAGEMENT CLIENTS

What steps can be taken to educate employees about fraud prevention?

- Create a training program focused on fraud education and the importance of safeguarding sensitive information.
- Promote a culture of fraud awareness to encourage staff to raise concerns.
- Establish an incident response process to deal with fraud events.
- Test employees with automatic phishing simulations.

What internal controls should organizations consider implementing?

General

- Create a standard operating procedure across all tasks.
- Establish a written code of conduct.
- Perform regular audits and control testing.
- Keep signature cards up to date.
- Ensure that the tasks of the payment process, such as preparation, approval and reconciliation, are separated among at least two employees.
- Limit access and resources for each job role.

Online

- Require dual approvals to authorize payment requests and user profile changes.
- Use different workstations for initiating and approving transactions.
- Enforce the use of unique user IDs along with complex passwords that include letters, numbers, and characters or a passphrase.
- Promptly remove or disable access for terminated employees.

Check

- Implement multi-level security features on checks, such as watermarks, holograms, or heat-sensitive ink.
- Securely store blank checks, signature stamps, and check printing equipment.
- Encrypt and password-protect check templates stored on digital devices.
- Conduct check inventory reviews regularly to account for all unused checks.
- Avoid placing checks in an unsecure mailbox or on your counter for the mail courier to pick up.

See back for legal and compliance disclosures.

What steps should be taken on new vendor requests?

- Complete a new vendor validation check before being entered into the system.
- Confirm and verify funds transfer/change requests by calling the vendor at a known phone number.

How can workstations be protected?

- Keep all workstations up to date: operating system, software, antivirus, and malware protection.
- Limit personal use on computers used for online banking activities.
- Regularly back up data on separate servers to protect against unexpected events.
- If possible, restrict the ability to install software to certain individuals such as IT Professionals.
- Always exercise caution when downloading applications, documents, installing software, or opening email attachments.

What measures should be taken when sending confidential data?

- Use encryption software to send confidential information securely.
- Truncate account numbers in communications.
- Always verify the recipients of communications before sending.

What proactive steps can be taken to monitor account activity?

- Monitor accounts daily and notify the bank immediately if suspicious activity is detected.
- Carefully review all bank statements.
- Activate necessary online banking alerts, such as account activity, added users, approval requests, and failed logins.

What are some other fraud protection steps that can be taken?

- Look at available insurance options for coverage against cybersecurity fraud and general fraud protection.
- Implement fraud protection on your bank accounts with Positive Pay services or Check or ACH Block.
- Limit check writing by implementing or increasing ACH originated payments.

Let's start a conversation

For additional information, visit us at **JohnsonFinancialGroup.com.**

JOHNSON FINANCIAL GROUP®