

Delivering Security Leadership – Audit Log Review

Security and fraud risks can come from inside companies as often as from the outside. Strong internal controls and policies, coupled with strong authentication, create multiple layers of security to help prevent fraud and safeguard your information. Your audit log review program is one of the most important weapons in your arsenal for protecting your company's assets.

Bank of America Direct® audit logs help you to identify unauthorized activities, detect suspicious behavior, reconstruct events and promote accountability.

Follow best practices for audit log review.

Experts agree that the most effective audit program is an integral, well-understood part of a company's business routine. Suggested practices include:

- Establish a regular schedule of review.
- Separate review responsibilities from entitlement and payment activities.
- Formalize escalation procedures for findings.
- Communicate the audit log review process to everyone in your company. Knowing that all actions are recorded and reviewed is a powerful fraud deterrent.

Enhance the value of your review by targeting key risk activities.

Watching administrative actions is equally important as monitoring money movement.

- Verify the creation of new users with appropriate entitlements.
- Delete IDs and entitlements promptly when users leave your company or change roles.
- Be suspicious of account logon failures, especially during non-business hours.
- Watch for repeated password changes.
- Pay careful attention to transaction activity that creates opportunities for financial loss.

Use checks and balances.

Engaging an independent party to review your security administrator's actions helps provide the necessary checks and balances for managing your company's system security.

Take full advantage of your system's features to strengthen your audit process.

Bank of America Direct audit tools allow you to expand or narrow the scope of your review according to your business parameters and analytical needs. Our system is designed to let you:

- View all users or a specific user for all activity or a specific activity.
- View a single account or application, or all accounts and applications.
- View activity for a single day or for a specific time frame.
- Generate custom or standardized reports.
- Obtain real time information.
- Access 90 days of historical data immediately.
- Retrieve up to seven years of data from taped archives for online viewing.
- Set up a user specifically for audit review.

For more information about Bank of America Direct security and audit controls, including terms and conditions that may apply, contact your Global Treasury Services representative. Also, visit us at www.bankofamerica.com.

Putting your Bank of America Direct audit logs to work.

Application	Critical Events	Description
Administration		
Check administration activities. <i>Click “Log” on the main Bank of America Direct menu bar.</i>	<ul style="list-style-type: none"> • Approve password change • Approve user entitlement • Initiate password change • Initiate user entitlement • Insert user 	<ul style="list-style-type: none"> • Administrative activities open the door to your systems and accounts. • Repeated administrator logon failures may indicate attempts to circumvent your company’s security settings. • Inappropriate requests or authorizations can lead to financial loss.
ACH		
Check money movement. <i>Select Admin from the ACH drop-down.</i> <i>Click the Audit Log Report tab.</i>	<ul style="list-style-type: none"> • ACH bath approval • ACH pass-thru 	<ul style="list-style-type: none"> • Approving a transaction or accepting a pass-thru file sends payments for processing. • Logs reveal the source ID for actions, but compromised IDs or inappropriate entitlements can slow progress in identifying potentially fraudulent activities.
FX Wires & Drafts		
Check money movement. <i>Select “Event Audit Report” under the FXWD Inquiry/Report heading.</i>	<ul style="list-style-type: none"> • Approve transaction 	<ul style="list-style-type: none"> • Approving a transaction releases the wire for processing. • Logs reveal the source ID for actions, but compromised IDs or inappropriate entitlements can slow progress in identifying potentially fraudulent activities.
Payments Initiation		
Check money movement. <i>Click “Log” on the main Bank of America Direct menu bar.</i>	<ul style="list-style-type: none"> • Approve payment • Release transaction (legacy Payments Initiation 2005) 	<ul style="list-style-type: none"> • Approving a payment or releasing a transaction sends payments for processing. • Logs reveal the source ID for actions, but compromised IDs or inappropriate entitlements can slow progress in identifying potentially fraudulent activities.
Positive Pay		
Check timeliness and accuracy of decisions. <i>Click “Log” on the main Bank of America Direct menu bar.</i>	<ul style="list-style-type: none"> • Release exception 	<ul style="list-style-type: none"> • Releasing an exception item sends the payment for processing. • Failure to provide timely decisions may result in financial loss and could indicate a weakness in your internal fraud prevention process. • Inaccurate pay or return decisions could signal internal fraud.
Reconciliation		
Check accuracy and promptness. <i>Click “Log” on the main Bank of America Direct menu bar.</i>	<ul style="list-style-type: none"> • Release issue 	<ul style="list-style-type: none"> • Adding a fraudulent check to your issue register could result in financial loss. • Failure to reconcile accounts promptly may result in financial loss and can undercut the effectiveness of your other fraud prevention tools.
Self-service password reset		
Check access changes and errors. <i>Click “Log” on the main Bank of America Direct menu bar.</i>	<ul style="list-style-type: none"> • All actions 	<ul style="list-style-type: none"> • Failed logins, failed password resets and failed helpdesk authentications or challenge questions may indicate attempts to breach your company’s accounts from the inside or the outside. • Repeated password resets may signal unauthorized access.

These steps to help mitigate fraud are suggestions only and are not a guaranty against fraud, and are not meant to substitute for your own internal procedures, which are appropriate for your company.