CIS Kenya

CIS Kenya ValiData Operational Guidelines

Embedding CIS ValiData Operations into CIP Processes

Contents

1. Introduction

The purpose of these guidelines is to assist Credit Information Providers (CIPs) in refining existing processes or establishing new processes tailored to the ValiData system. They are primarily relevant for credit operations, information technology, risk management, data governance, and regulatory compliance teams within a CIP. CIS Kenya, a non-profit member-based association is the owner of the ValiData system.

2. Technical Support

CIS Kenya will offer technical support to CIPs experiencing challenges with ValiData that cannot be resolved internally. To ensure timely response and effective resource allocation, please follow these procedures:

Contact Information - This information is also available within the Help tab of the ValiData system**:**

- Dedicated support email address: **technicalservices@ciskenya.co.ke**
- Dedicated support phone number: **+254 714917370**
- Website: **https://ciskenya.co.ke/validata/**

Issue Classification and Resolution Timelines:

- **High Impact** (Complete system failure, security breach): Resolution within 2 hours
- **Medium Impact** (Consistent malfunction, inability to submit to a CRB): Resolution within 12 hours
- **Low Impact** (Isolated feature issues): Resolution within 24 hours

Issue Reporting - Submit the following details to expedite troubleshooting:

- Date and time the issue first occurred
- Detailed description of the problem
- Exact steps to reproduce the error
- Error messages and screenshots (include the URL in the screenshot)
- Consider adopting the following table:

Date Issue Noted:		**Time Issue Noted**	
Detailed description of the problem:			
Exact sequence of steps to reproduce the error:			

Description of failure and/or error message:
Insert screenshot (ensure screenshot displays the URL)**:**

3. User Account Management

To maintain user access control and system integrity, CIPs should implement these procedures for user account management on ValiData:

User Creation:

As part of their own internal user creation processes, a CIP should adopt the following as minimum requirements to set a user up on the ValiData

- Formal request process with designated approver for a user to be created
- Defined user roles and access levels aligned with job functions
- Standard information requirements for new user requests

User Onboarding:

- Users should be provided with mandatory induction training on the tool's functionality inclusive of reporting capabilities which can be found in the User Training Manual, and the supporting operational processes and relevant regulatory policies of the CIP.
- Customize the quick reference guides in appendix to CIP standards and issue to new user.

Account Suspension & Termination:

- Suspending a User Account:
  - Identification of User for Suspension:

- A user going on extended leave of absence fills in a leave form for approval by the line manager and HR representative as is relevant to the CIP's policies and processes. Once its duly signed, the form is handed over to the systems administrator.
- Extended leave could arise from situations such as maternity/paternity leave, medical leave, sabbatical, or other long-term absences.

- Account Suspension Notification:
  - The system administrator sends a notification to the user informing them that their ValiData account (and other system access they have) will be temporarily suspended due to their extended leave.
  - The notification should include the expected duration of the suspension and instructions for reactivating the account upon their return.
- Account Suspension:
  - The system administrator logs into the ValiData admin console and locates the user's account.
  - The administrator changes the user's status to "Suspended" and saves the changes.
  - This will prevent the user from logging into the ValiData system until the account is reactivated.
- Access Revocation:
  - The system administrator revokes the user's access to any shared drives, folders, or other ValiData-related resources.
  - This ensures that the user cannot access or modify any data during their absence.
- Reactivation Upon Return:
  - When the user returns from their extended leave, they should notify the system administrator.
  - The administrator will locate the user's account, change the status back to "Active," and restore their access to ValiData resources.
  - The user should be informed that their account has been reactivated and they can resume normal usage of the ValiData system.

- Terminating a User Account Upon Employment Separation:
  - Identification of Terminated User:
    - HR department notifies the system administrator that an employee has been terminated or has voluntarily left the organization.
  - Account Termination Notification:
    - The system administrator sends a notification to the line manager of the informing them that the ValiData account of terminated user is to be permanently deactivated.

- The notification should include the effective date of the account termination.

- Account Deactivation:
  - The system administrator logs into the ValiData admin console and locates the user's account.
  - The administrator changes the user's status to "Terminated" and saves the changes.
  - This will prevent the user from logging into the ValiData system.
- Access Revocation:
  - The system administrator revokes the user's access to any shared drives, folders, or other ValiData-related resources.
  - This ensures the terminated user cannot access or modify any ValiData data.
- Data Retention:
  - The system administrator should ensure that ValiData access logs associated with the terminated user are appropriately archived or backed up for future reference.
  - The CIP's data retention policies should be followed to determine the appropriate duration for retaining the terminated user's data.
- Confirmation of Termination:
  - The system administrator should confirm the account termination with the HR department or the user's manager to ensure the action was taken correctly.

4. Tool Update and Change Management

CIS Kenya, in collaboration with the industry's Technical Working Group (TWG), periodically proposes updates to the ValiData system or reporting templates. These proposed changes are then subject to review and approval by the Central Bank of Kenya (CBK). Once approved, CIS Kenya will inform CIPs of the planned changes and their effective dates. Some of these updates may necessitate adjustments to how files are extracted or prepared from the CIPs' reporting Management Information Systems (MIS). CIPs should proactively assess the potential impacts on their internal data extraction or preparation processes when planning for these updates:

Approval Process:

- Require formal requests outlining the change details, impact analysis, and testing guidelines as needed from CIS Kenya
- Have the internal CIP Change Control Board or the designated responsible staff review and approve updates for testing.
- CIP Change Control Board or the designated responsible staff assigns staff to implement impacted areas internally and test the changes in safe UAT virtual machine environment
- CIP Change Control Board or the designated responsible staff approves for the changes to be implemented in production virtual machine

Change Communication:

- The Change Control Board or designate responsible staff to provide advance notice to all users about scheduled updates and any planned downtime.
- Clearly communicate changes, new features, and potential impacts for a smooth transition.

5. Incident Reporting and Monitoring

CIPs should have a well-defined procedure for reporting and monitoring incidents related to ValiData to protect system and data integrity.

- **Incident Definition:** Clearly define reportable incidents (e.g., data breaches, unauthorized access, system malfunctions, extended downtime).
- **Reporting Procedure:**
  - Designate a contact or team for incident reporting
  - Establish reporting timelines (especially for critical situations)
  - Provide a standard incident report form/template.
- **Monitoring:**
  - Implement regular system health checks to proactively identify potential issues.
  - Regularly review the incidents reported to establish trends, patterns and root causes

6. Resolution of Validation Errors

Reports are generated by ValiData tool as part of the outputs. It is important to note that these reports remain on the system for a period of 24 hours only. A robust process is therefore required for downloading the file and handling validation errors to ensure data quality and timely regulatory reporting. CIPs should implement the following:

- **Error Handling Process:** Develop a detailed process that includes:
  - Identifying failed validation records/files
  - Investigating the root cause e.g., data quality issues, extraction logic errors, ValiData tool bugs.
  - Internally implementing corrective actions (at the data source or extraction level), and escalating incidences where action is required at the vendor level e.g. bugs as per the technical support section above
  - Prioritizing and tracking resolution
- **Documentation:** Emphasize the importance of documenting corrections, including the reason for the change and the date it was made for audit purposes.

7. Conclusion

These guidelines are indicative, recommendations by which the CIP can opt to align its specific policies and processes with. Since ValiData processes likely intersect with multiple operational areas, involve all relevant internal stakeholders (credit operations, IT, risk management, data governance, and regulatory compliance) when refining and documenting your internal processes.

Appendix

ValiData Quick Reference Guide

Logging In

1. Navigate to the ValiData login page.
2. Enter your registered email address and password.
3. Click the "Login" button.

Validating Data

1. Click on the "Upload Files" option in the side navigation.
2. Select the appropriate subscriber from the dropdown menu.
3. Click the "Choose Files" button and select the file(s) you want to validate.
4. Select the template version.
5. Click the "Upload" button to start the validation process.
6. Check the "View Upload Status" link to monitor the validation progress and view any error logs.

Viewing Error Logs

1. Click on the "View Files" option in the side navigation.
2. Locate the file you want to view the error log for and click on the file name.
3. Review the error summary and the detailed error log table.
4. Apply filters to find specific errors if needed.
5. Click the "Download" button to export the error logs as a CSV file.

Submitting Files to the CRB

1. Go to the "View Files" page.
2. Select the file(s) you want to submit by checking the corresponding checkbox(es).
3. Click the "Submit" button.
4. Choose to submit to all available CRBs or select a specific CRB using the "Advanced Options".
5. Click "Submit" to complete the process.

Monitoring Submitted File Status

1. Navigate to the "View Submissions" page.
2. Review the list of submitted files and their respective statuses.
3. Use the pagination and filtering options to find specific submissions.

Administering the System

1. Click on the "Create and Manage Users" option in the side navigation.
2. To create a new user, click the "Create User" button and fill in the required information.
3. To manage user roles, click on the "Add roles to a user" button.
4. Use the "Manage Settings" option to modify subscriber settings, create/manage CRB profiles, and manage notification settings.
5. Explore the "Manage General Settings" section to view system statuses, check for updates, and control server settings.

Remember, this is a quick reference guide, and you should refer to the full user manual for more detailed instructions and information on all the features and functionalities of the ValiData application.