

\$ Jimwe Tiljok im Mol \$

Public Financial Management – Ministry of Finance

8.1 Bisan User Access Controls

VERSION 1.0 OCTOBER 2022

Table of Contents

1. Objective	2
2. GRMI Scope	2
3. Authority	2
4. Workflow/Process Flowchart	2
5. Detailed Process Procedures	3
6. Accounting Entries in BISAN	11

1. Objective

The objective of this module is to explain how the Bisan Financial Management Information System (FMIS) controls user access to the system.

Controlling user access to the FMIS system is an integral part of the overall budget execution and financial reporting and control process. It is specific to the GRMI financial accounting/financial management policies and procedures.

As with all other modules in this policy and procedures manual, it starts with a schematic overview of the process then discusses each step in detail, highlighting the screens and approvals required at each step

2. GRMI Scope

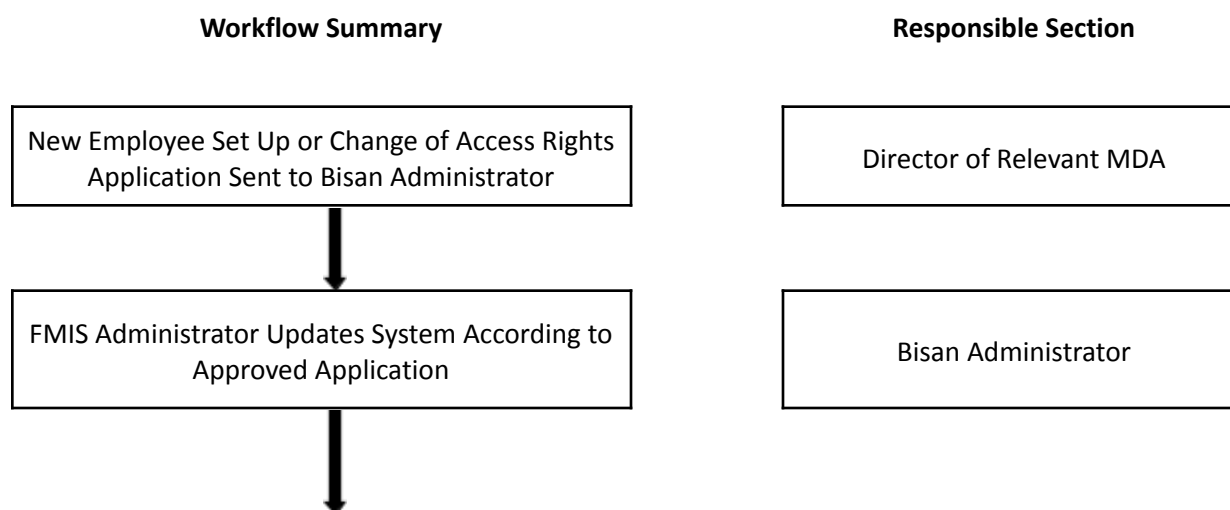
This procedure is of interest to:

- System Administration

3. Authority

Because the Ministry of Finance is charged with maintaining the integrity of the accounting system, they must ensure access to the journals of original entry is well controlled. It is from this overall requirement that the authority for this Module is derived. User access controls are changed/updated by the System Administrator; however, the System Administrator must receive authorization from the ---*Please specify as required* before changes can be made. These changes are logged and files kept for all authorizations. See **Appendix A** for an example of the **User Access Maintenance Form** that is filed for documentation purposes.

4. Workflow/Process Flowchart



Approved Application Filed by System
Administrator

Bisan Administrator

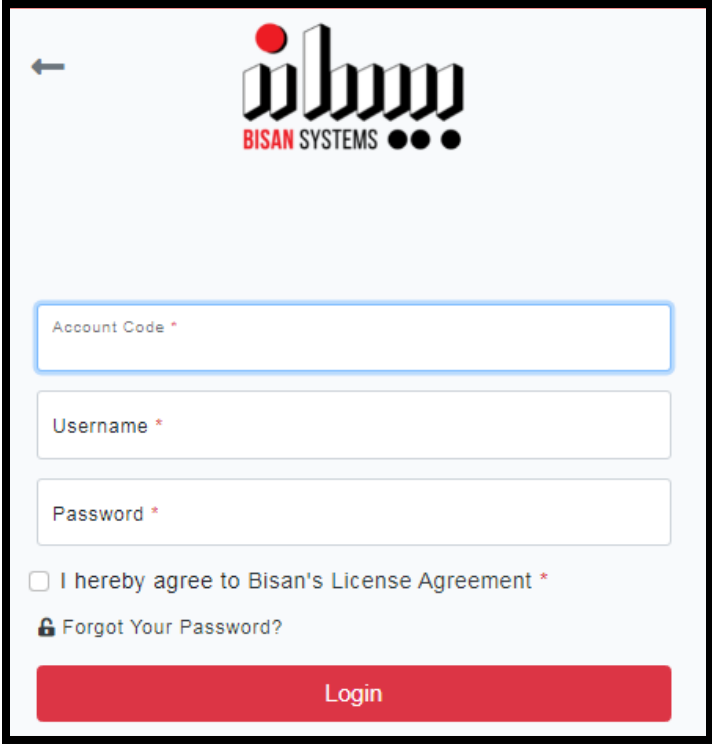
5. Detailed Process Procedures

With a computerized budget control, accounting and payment system, it is essential that a robust user security system be in place within the Bisan FMIS system to maintain the integrity of the financial data and ensure unauthorized entries are not made. The following is a summary of the key security features of the Bisan system. The system administrator is the only person who has access to the system to change and set up user security.

System Access

When accessing the system, each user has a unique **Username** and **Password**. The username and password is given by the Bisan system administrator and when the user first logs onto the system, they are prompted to change their password. The password must be at least 5 characters in length and should be a combination of letters and numbers. The password is case sensitive. The system also automatically requires the users to change their passwords regularly. The length of time is determined by the system administrator and the current norm for the GRMI is every 60 days. When logging into the system and the allotted time has expired, before proceeding any further, the user must change their password. A password history is also maintained in the system so the user cannot switch between two passwords all the time.

To sign onto the system, you will immediately be shown the following screen:



←

BISAN SYSTEMS

Account Code *

Username *

Password *

☐ I hereby agree to Bisan's License Agreement *

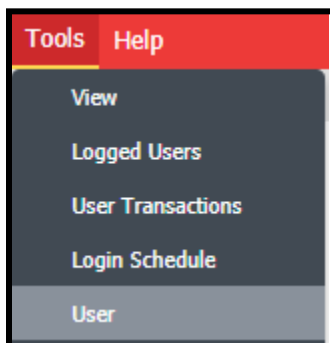
[Forgot Your Password?](#)

Login

Type in your **Account Code**, **Username** and **Password**, check the box to agree to License Agreement, and click **Login**.

For the system administrator to create a Username and Password, they would perform the following steps.


Navigate to the User screen:



This will then open a table listing all users, a sample of which is shown below:

User (Enabled)					
<div> Refresh Print Export Import Undo Redo User Preference Help Share Enabled Grid </div>					
Search <input type="text" value="Search Keyword"/> <input type="text" value="Contain"/> <input type="text"/> <input type="button" value="Search"/>					
Username	Full Name	Enabled	Used	Last Password Change	
ADMIN	Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30/08/2021 01:49:50	
USER1	user1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	28/09/2021 08:26:38	
USER2	user2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	28/09/2021 08:26:57	

Based on the above screenshot, you can determine some important information with respect to the last time the password was changed and whether the user is active and has used the system.

To set up a new user, the system administrator would then click on the Add button  and the following screen appears that must be completed:

The screenshot displays the 'General' tab of a user management interface. At the top, there's a header 'User : TEST - test' and a toolbar with icons for save, print, refresh, delete, clock, mail, document, and a 'User Preference' button. Below the toolbar are four tabs: 'General' (selected), 'Access Group', 'Advanced', and 'API'. The 'General' tab contains the following fields and controls:

- Username:** TEST (text input), with checkboxes for **Enabled** and **Used**.
- Full Name:** test (text input), with language dropdowns for **English** and **español**.
- Login Access:** Normal (dropdown menu).
- Authentication Through:** Bisan (dropdown menu).
- Last Password Change:** 10/06/2022 11 (text input).
- Last Login:** 10/06/2022 12 (text input).
- Login Schedule:** (text input), with checkboxes for **Never disconnect user** and **Password Never Expires**.
- Employee:** 1 (text input).
- Station:** 000000002 (text input).
- Location:** (text input).

The above section is very self-explanatory and shows how the user can be set up and controlled. Of particular importance are the two tabs at the top of the User screen, **Access Group** and **Advanced**, as this allows the level of access control, which will be explained in the following sections. The overall goal of setting up a user can be understood in the following 3 steps:

1. Once user is set up, assign a functional access group(s) to the user depending on their job function/role.
2. Once a user is set up and functional access group(s) has been assigned, the next step is to specifically define what they can see/access within the whole of government when performing their functional job specifications. This is sometimes called User Group access. In Bisan, it is part of “Advanced” security.

The following sections describe Functional Access Group definition and Advanced Security (User Group Access).

Functional Access Group

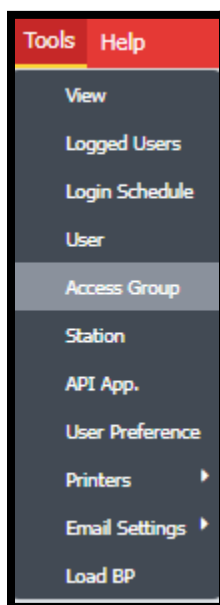
This is a separate authorization based on the function/role of a particular set of employees. For example, the Data Entry person for Payment Vouchers, Supervisor who reviews the data entry of the person who enters Payment Vouchers, Department Head, etc. are treated as separate Functional Access Groups. Each separate Functional Access Group is allowed to perform certain functions and only those functions (full access or restricted access). This is an effective way to ensure that only authorized personnel perform certain functions, and it ensures adequate segregation of duties. There can also be certain Functional Access Groups that are given to staff who just need to create and view reports and not enter data, for example. Functional Access Groups are limited by one’s imagination only. Once these groups are established and defined, they are then “attached” to individual users. Users can have one or more of these Functional Access Groups assigned to them.

The following is an example of some Functional Access Groups that are set up in the GRMI Bisan system with respect to creating/saving/approving a budget voucher, along with a short explanation of the rights and duties of each group:







Functional Group	General Duties and Rights
BVCREATE	To add a budget voucher (original budget set up, supplementary budget and save)
BVREVIEW1	To review a saved budget voucher, accept or reject and post


For the system administrator to create Functional Access Groups, they would perform the following steps:

Navigate to the Access Group screen:









This will then open a table listing all Access Groups already created in the system, an example of which is shown below related to the GRMI:

Access Group (Enabled)	
     	
Search	<input type="text" value="Search Keyword"/> <input type="button" value="Contain"/>
Code ↑	Name
BRVCREATE	Commitment Voucher Creation
BRVFINALIZE	Commitment Voucher Finalize
BRVIEWONLY	Budget Request Voucher View Only
BUDGETCREATION	New Budget Creation
BUDGETVCREATE	Budget Voucher Create
BUDGETVFINALIZE	Budget Voucher Finalize
COLLECTIONRPT	Collection Reports
CREATEJV	Create Journal Voucher
CREATEVENDOR	Create Vendor EIN/ Employee SS

If the Administrator wants to add a new Access Group, they will click on the Add button  and the following screen would appear that needs to be completed according the requirements of the Access Group:

New Access Group :

Code
☒ Enabled
☐ Used
☐ Header

Name español

English

Tables

Reports

Fields

Others

Table	Command	Enabled
1 API App.	1 View	<input type="checkbox"/>
2 AR/AP Settlement		
3 Access Group		
4 Account		
5 Area		
6 Asset		
7 Asset Family		
8 Auditor Code		
9 Bad Credit Account		
10 Bank Check		
11 Bank Deposit Voucher		
12 Bank Ledger		
13 Bank Print Formats		
14 Bank Transfer		

After entering a unique Code for the Access Group and naming it, the next job for the Administrator is to define what can be done by that group using the various **Table**, **Report** and **Field** tabs.

First step: Choose the Tables that must be activated for this user to view. Once a table is chosen

Enabled

by clicking on the Enable checkbox ☒, the table will automatically expand to give the Administrator greater scope to set up the Access Group as desired (Command column is active). For example, if the Budget table is enabled, the following expanded choices will open:

Tables Reports Fields Others			
Table		Command	Enabled
15	Banks & Branches List	1 View	<input checked="" type="checkbox"/>
16	Book	2 Modify	<input type="checkbox"/>
17	Budget	3 New	<input type="checkbox"/>
18	Budget Control	4 Print	<input type="checkbox"/>
19	Budget Ledger	5 Clone Original	<input type="checkbox"/>
20	Budget Reallocation	6 Delete	<input type="checkbox"/>
21	Budget Summary	7 Print List	<input type="checkbox"/>
22	Budget Voucher	8 Export List	<input type="checkbox"/>
23	Category	9 Email List	<input type="checkbox"/>
24	Check Info	10 History	<input type="checkbox"/>
25	Commitment Voucher	11 Email	<input type="checkbox"/>
26	Component	12 Budget Voucher	<input type="checkbox"/>
27	Contact Info	13 Budget Reallocation	<input type="checkbox"/>
28	Contact Map	14 Funds Release	<input type="checkbox"/>
29	Cost Center	15 Funds Reallocation	<input type="checkbox"/>
30	Country	16 Budget Summary	<input type="checkbox"/>
31	Country Category	17 Report	<input type="checkbox"/>

From here, the Administrator can define whether there is View only access or whether additions, edits, posting, printing, etc. are allowed.

Second Step: After choosing the correct tables the Access Group can access (remember when defining the User Access controls earlier, they can be limited to only one organization, therefore, the tables being accessed above would only apply to information for that particular organization depending on how it is defined in the User Group or Advanced security), you can define the specific fields that are enabled, disabled or hidden. This allows specific control of the use of a particular voucher based on the access group.


Third Step: A next step would be to define the reports that this particular Access Group can view. A screenshot below is given to show how certain reports can be **enabled** for an Access Group:

Code: ☒ Enabled ☒ Used ☐ Header

Name:

Tables Reports Fields Others

	Command	Enabled
1	Account Against Detail	<input type="checkbox"/>
2	Account Against Summary	<input type="checkbox"/>
3	Adjusted Trial balance	<input type="checkbox"/>
4	Adjustment Journal Report	<input type="checkbox"/>
5	Aggregated Funds Release	<input type="checkbox"/>
6	Auditor Trial Balance	<input type="checkbox"/>
7	Balance Sheet	<input type="checkbox"/>
8	Bank Account Balances	<input type="checkbox"/>
9	Budget Detail	<input checked="" type="checkbox"/>
10	Budget Documents Tracing	<input type="checkbox"/>
11	Budget Report	<input checked="" type="checkbox"/>
12	Budget Segmented Report	<input checked="" type="checkbox"/>
13	Budgeted vs. Actual Payments	<input type="checkbox"/>
14	Canceled Documents	<input type="checkbox"/>
15	Canceled Documents Detail	<input type="checkbox"/>

Once you have chosen which reports the functional group can access, Click **Save** .

Assigning Functional Access Groups to Users:

To assign a Functional Access Group to a particular User, the Administrator would perform the following steps:

Navigate to the following screen, as explained earlier:

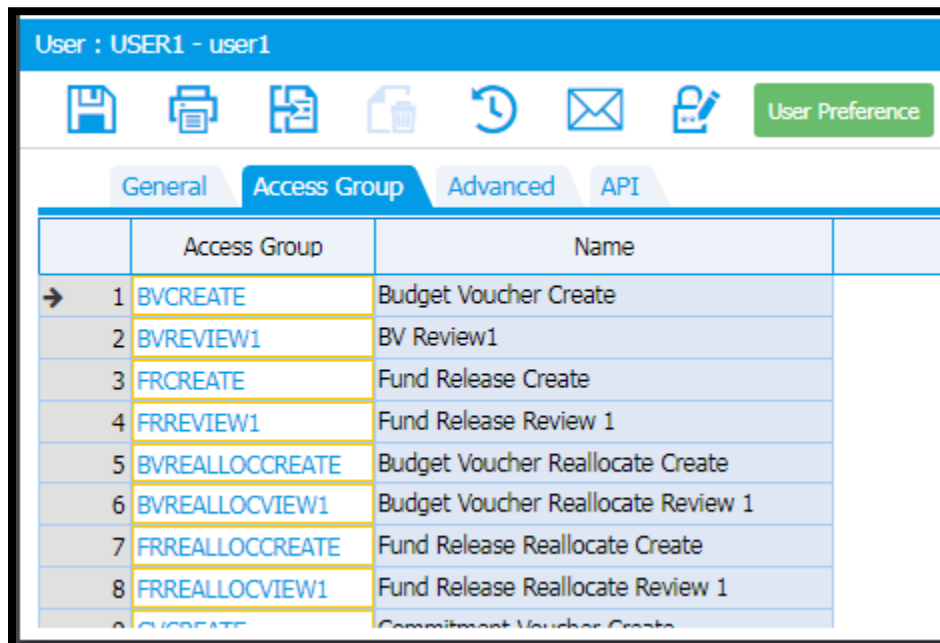
User (Enabled)

Search:

Username	Full Name	Enabled	Used	Last Password Change
ADMIN	Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30/08/2021 01:49:50
USER1	user1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	28/09/2021 08:26:38
USER2	user2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	28/09/2021 08:26:57

Double-click on the User you want to attach Access Groups to and open the user. From here, click on the "Access Group" tab and this will display enabled access groups already attached to this user. You can double-click on the Access Group field and scroll through the groups you have

set up separately then attach the group to the user. You can attach multiple groups to this user or remove groups as required.

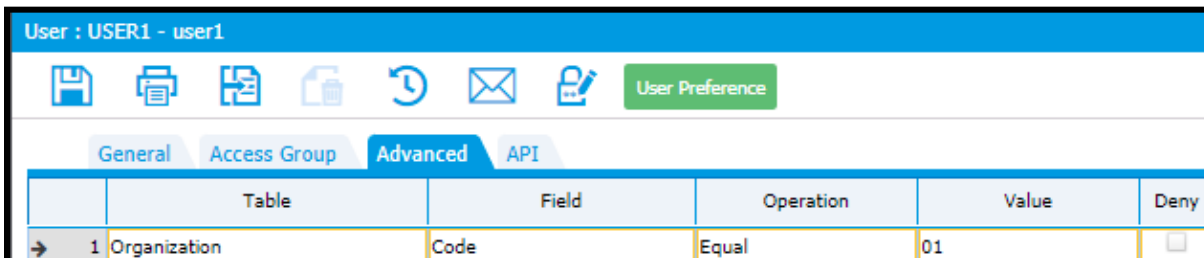


User Access – Advanced Tab

This tab allows the administrator to define access by table and field within the tables. For example, define users to see information only within their particular Organization or Department of their Organization. As an example, budget employees assigned to the specific organization can **ONLY** view and make changes to their Organization’s data. Likewise, certain users may also be further restricted to certain departments within the organization. It all depends on the level of restriction required by the Ministry of Finance (or when decentralized, the particular Minister within their Ministry). They cannot view or make changes to any other Organization. Alternatively, some users, like the Director of Budget, can see all Organizations given that he/she must approve all budget vouchers for GRMI as a whole. This “full” access feature is limited to a few Staff and is strictly controlled by the System Administrator.

For the system administrator to create User Access, they would perform the following steps:

Navigate to the following screen for the User and activate the advanced tab:



From here, define which tables and which fields to which the person has access. Based on the above example, user1 is able to access organization 01 **only** and what he can access and undertake will depend on his functional access group rights. If the advanced user rights tab is left blank for the user, there are no special restrictions, and the user can access all entities and functions based on the access group assigned. If user1 was to have a certain entity restricted out of the total, the “deny” check box would be ticked. Do note that this advanced tab allows very powerful control over user access rights and it is not limited to organization as this simple example show above. This tab can control most fields of all tables that the user can access.

Click **Save**.

Approval Levels for Voucher Processing

Apart from assigning a Functional Access Group to a particular user and defining Advanced User Access rights, there is also added control of establishing the **levels of approval** that each Functional Access Group has when creating and authorizing vouchers in the system and the various levels and sequence of authorization required (workflow). For example, the business process for creating a Payment Voucher and processing it through to being able to be paid requires that there are **two** separate levels of electronic approval BEFORE the voucher can be paid (posted).

The following screenshot is an example of the two levels of approval for the Payment Voucher:

	Level	Accept Group	Reject Group	Required	Lock	Auto Send	Level On Reject
1	Entry	PVCREATE		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
2	APPROVAL1	PVREVIEW1	PVREVIEW1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Entry
3	APPROVAL2	PVFINALIZE	PVFINALIZE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Entry
4	Posted	PVFINALIZE	PVFINALIZE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Entry
5	Delivered	PVFINALIZE		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

In the above, you will note that there are mandatory GRMI levels of approval as shown in the “Level” column, APPROVAL1 and APPROVAL2 before Posting.

The Approval Levels are separately defined in Bisan. These approval levels are then assigned to an Approve Group. Those that have been assigned that Group can approve at the level indicated. Likewise, these levels can also be assigned to a certain group that has the right to reject prior approvals.

6. Accounting Entries in BISAN

None, no GL impact