

Segregation of Duties

Fiscal Year 2014 Finding Summary

External Auditor Results for Fiscal Year 2014 (July 1, 2013 thru June 30, 2014)

- Total number of findings up 123% from 13 in FY13 to 29 in FY14
- Financial Statement findings up 20% from 5 in FY13 to 6 in FY14
- **Federal/Financial Aid findings up 188% from 8 in FY 13 to 23 in FY 14**

Ineffective Logical Access Controls (7)

Definitions:

Separation of duties: (SoD) (also known as "Segregation of duties") is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task is an [internal control](#) intended to prevent [fraud](#) and [error](#).

Logical Access: In information technology, **logical access controls** are tools and protocols used for [identification](#), [authentication](#), [authorization](#), and [accountability](#) in [computer information systems](#).

Resource Management: In [organizational studies](#), **resource management** is the efficient and effective deployment of an organization's resources when they are needed. Such resources may include financial resources, inventory, human skills, production resources, or information technology (IT).

DOAA SOD Matrix

Creating A More Educated Georgia

USG Templates

Creating A More Educated Georgia

Georgia *FIRST*:

Auditing – Segregation of Duties

- The SEGREGATE_DUTY_BOR is a very important query with which security administrators on campus should become familiar. This query uses the Segregation of Duties Matrix that was provided by the auditors and displays users that have potential or real segregation of duties issues. The results on this query will need to be reviewed, and administrators need to have the appropriate reasons documented and signed off on for the auditors.
- A job aid for this query is available on the Georgia*FIRST* website at http://www.usg.edu/gafirst-fin/documentation/job_aids/category/security

				<div><div>Create Requisition</div><div>Approve Requisition</div><div>Create PO</div><div>Approve PO</div><div>Create Voucher</div><div>Approve Voucher</div><div>Cut Check</div><div>Add/Edit Vendor</div><div>Approve Vendor</div><div>Bank Reconciliation</div><div>Enter JE</div><div>Approve JE</div><div>Custody of Cash</div><div>Approval of Bank De</div><div>Post Receipts</div><div>Add/Edit Customers</div><div>TGRRCON (BANNE</div><div>Hire Employee</div><div>Change Compensation</div><div>Change Benefits</div><div>Create Paycheck</div><div>ADP Recon</div></div>																					
Process	COSO	Procedure/Function	Grp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Purchasing	R	Create Requisition	1		X		*		*	X	X	X	X		*										
	A	Approve Requisition	2	X		*		*		X	X	X	X	*											
	R	Create PO	3		*		X		*	X	X	X	X		*										
	A	Approve PO	4	*		X		*		X	X	X	X	*											
	R	Create Voucher	5		*		*		X	X	X	X	X		*										
	A	Approve Voucher	6	*		*		X		X	X	X	X	*											
	C	Cut Check	7	X	X	X	X	X	X		X	X	X	X	X										
	A	Add/Edit Vendor	8	X	X	X	X	X	X	X		X													
	A	Approve Vendor	9	X	X	X	X	X	X	X	X														
Reconciliation	RX	Bank Reconciliation	10	X	X	X	X	X	X	X				*	X	X	X	X						X	
Journal Entry	R	Enter JE	11		*		*		*	X			*		X	X	X	X							
	A	Approve JE	12	*		*		*		X			X	X		X	X	X							
Cash Receipts	C	Custody of Cash	13										X	X	X		X	X	X	X		X	X	X	
	A	Approval of Bank Deposit	14										X	X	X	X		X	X	X					
	R	Post Receipts	15										X	X	X	X	X		X	X					
	A	Add/Edit Customers	16													X	X	X		X					
	RX	TGRRCON (BANNER)	17													X	X	X	X						
Emp Comp	R	Hire Employee	17																			X	X	X	X
	A	Change Compensation	18													X					X			X	X
	A	Change Benefits	19													X					X				X
	C	Create Paycheck	20										X			X					X	X			X
	RX	ADP Recon	22																		X	X	X	X	
				Purchasing									5	Journal			Cash Receipts				Employee Comp				

COSO Category	
R	Record
A	Authorize
C	Custody
RX	Reconcile

SOD Risk Level	
X	Elevated Risk
*	Low Risk

Auditing Controls

Limit Privilege Functions to appropriate personnel

- Review your security administrators on campus.
- Look at users with full access.
- Do users have access to system utilities/resources such as database tools, sql tools and crystal reports?

Auditing Controls

Local Security Administration - Maintain Segregation of Duties by separating the following roles:

- Requesting Access
- Approving Access
- Setting up Access
- Monitoring Access and Violations
- Performing Rights as a privileged user, and
- Monitoring a privileged user

Ensure Appropriate User Access and Authorization

- Is there an authorization form on file with the appropriate approvals in place?
- Are these periodically reviewed for changes or updates?
- Are terminated employee accounts locked or removed? (BOR_SEC_TERMINATED_USERS)
- Are user accounts reviewed for segregation of duties issues?

Auditing – Local Security Admins & IT Audit Packet

- *Campus Security Guide* contains campus security tools, processes, and queries that will assist identification of potential audit issues. This guide is posted as a zip file on the GeorgiaFIRST website and contains the following documents:
 - GeorgiaFIRST PeopleSoft Financials Campus Audit Packet
 - Local Security Administrator Responsibilities
 - Checklist for Audit
 - Segregation of Duties (SOD) Matrix
- Access the *Campus Security Guide* directly on the Security Job Aids and Reference Documentation webpage on the GeorgiaFIRST website:
http://www.usg.edu/gafirst-fin/documentation/job_aids/category/security

Security Queries

BOR_PORTAL_PERMISSIONS	Role page permissions with Functional name
SEGREGATE_DUTY_BOR	Segregation of Duties Query
BOR_SEC_ROLE_USERS	Users assigned to Role
BOR_SEC_TERMINATED_USERS	Security of Term'd Users
BOR_SEC_USER_PAGE	User ID page access
BOR_SEC_USER_PERM_LIST	Users and Permission Lists
BOR_SEC_USER_ROLES	User's Roles
BOR_SEC_USER_ROLE_PLIST_PAGE	Security Query

How to Piece it All Together

Start with the Segregate
Duty Bor Query

Pick a specific
Function/Process from the
Audit SOD Matrix

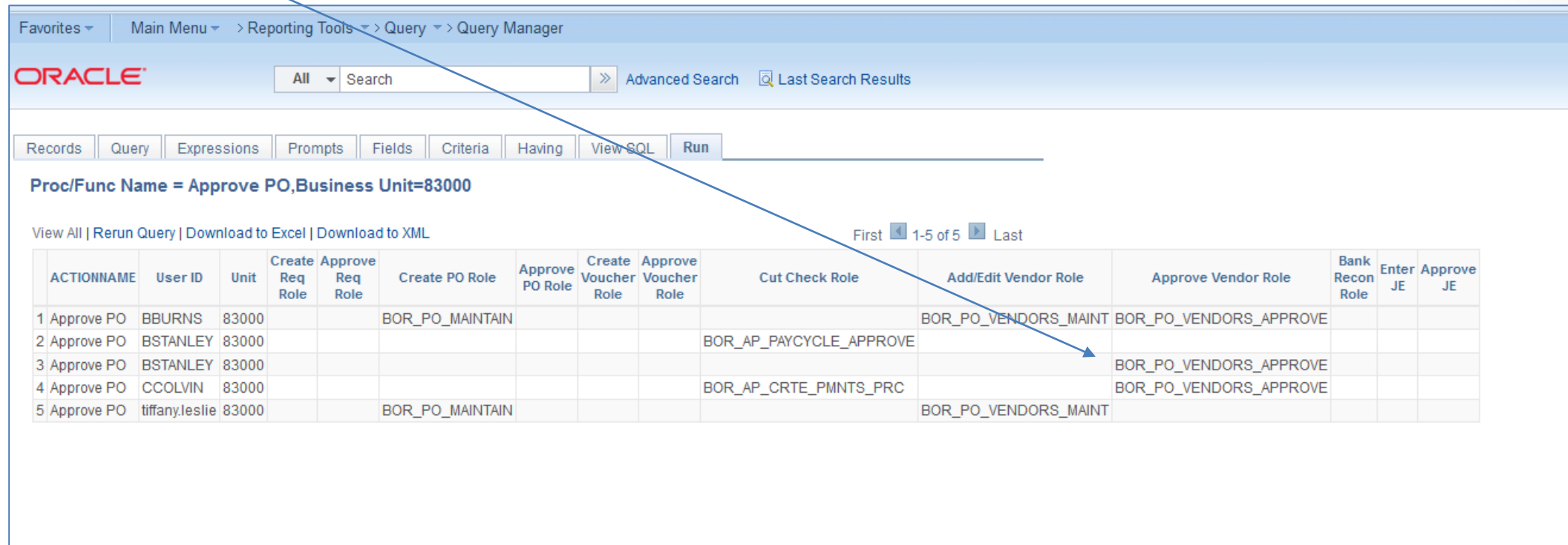
The screenshot shows the Oracle Query Manager interface. The query name is 'SEGREGATE_DUTY_BOR' and the description is 'Segregation of duties query'. The 'Fields' tab is selected, showing a list of fields with columns: Col, Record, Fieldname, Format, Ord, XLAT, Agg, Heading Text, Add Criteria, Edit, and Delete. The fields are numbered 1 through 15. A modal dialog is open over the 'Add Criteria' column for row 13, titled 'SEGREGATE_DUTY_BOR'. It contains two input fields: 'Proc/Func Name' with the value 'Approve PO' and 'Business Unit' with the value '83000'. There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

Col	Record	Fieldname	Format	Ord	XLAT	Agg	Heading Text	Add Criteria	Edit	Delete
1	A	A.ACTIONNAME - Action Name	Char30	1			ACTIONNAME		Edit	
2	A	A.ROLEUSER - User ID	Char30	2			User ID		Edit	
3	C	C.BUSINESS_UNIT - Business Unit	Char5				Unit		Edit	
4	A	A.ROLENAME - Role Name	Char30				Create Req Role		Edit	
5	A	A.ROLENAME2 - Role Name 2	Char30				Approve Req Role		Edit	
6	A	A.ROLENAME3 - Role Name 3	Char30				Create PO Role		Edit	
7	A	A.ROLENAME4 - Role Name 4	Char30				Approve PO Role		Edit	
8	A	A.ROLENAME1_BOR - BOR Role1	Char30				Create Voucher Role		Edit	
9	A	A.ROLENAME2_BOR - BOR Role2	Char30				Approve Voucher Role		Edit	
10	A	A.ROLENAME3_BOR - BOR Role3	Char30				Cut Check Role		Edit	
11	A	A.ROLENAME4_BOR - BOR Role4	Char30				Add/Edit Vendor Role		Edit	
12	A	A.ROLENAME5_BOR - BOR Role5	Char30				Approve Vendor Role		Edit	
13	A	A.ROLENAME6_BOR - BOR Role6	Char30				Bank Recon Role		Edit	
14	A	A.ROLENAME7_BOR - BOR Role7	Char30				Enter JE		Edit	
15	A	A.ROLENAME8_BOR - BOR Role8	Char30				Approve JE		Edit	

Reviewing the Results

If the user has the Role to Approve a Purchase order then the roles that have a 'POTENTIAL' segregation of duties risk are shown here.

This doesn't mean there is a Real Issue; You have to consider user preference controls and other controls the institution has in place.



Oracle Query Manager interface showing query results for 'Approve PO, Business Unit=83000'. The interface includes a navigation bar with 'Favorites', 'Main Menu', 'Reporting Tools', 'Query', and 'Query Manager'. A search bar with 'All' and 'Search' is present. Below the search bar, there are tabs for 'Records', 'Query', 'Expressions', 'Prompts', 'Fields', 'Criteria', 'Having', 'View SQL', and 'Run'. The query results are displayed in a table with 15 columns: ACTIONNAME, User ID, Unit, Create Req Role, Approve Req Role, Create PO Role, Approve PO Role, Create Voucher Role, Approve Voucher Role, Cut Check Role, Add/Edit Vendor Role, Approve Vendor Role, Bank Recon Role, Enter JE, and Approve JE. The results show 5 rows of data, all for 'Approve PO' actions. A blue arrow points from the text 'shown here.' to the table.

	ACTIONNAME	User ID	Unit	Create Req Role	Approve Req Role	Create PO Role	Approve PO Role	Create Voucher Role	Approve Voucher Role	Cut Check Role	Add/Edit Vendor Role	Approve Vendor Role	Bank Recon Role	Enter JE	Approve JE
1	Approve PO	BBURNS	83000			BOR_PO_MAINTAIN					BOR_PO_VENDORS_MAINT	BOR_PO_VENDORS_APPROVE			
2	Approve PO	BSTANLEY	83000							BOR_AP_PAYCYCLE_APPROVE					
3	Approve PO	BSTANLEY	83000									BOR_PO_VENDORS_APPROVE			
4	Approve PO	CCOLVIN	83000							BOR_AP_CRTE_PMNTS_PRC		BOR_PO_VENDORS_APPROVE			
5	Approve PO	tiffany.leslie	83000			BOR_PO_MAINTAIN					BOR_PO_VENDORS_MAINT				

Reviewing the Results

In this instance, BSTANLEY can Approve Purchase orders. However he cannot enter them, He can Approve Paycycles, but not run them, and He can approve vendors but not enter them. Therefore he can't enter a vendor and approve it, and create a voucher and pay it. Therefore there is no risk with this user id.

The screenshot displays the Oracle Procurement User Preferences interface for user BSTANLEY (Brian Stanley). The main page shows various search filters and a grid of authorization options. A modal window titled "Supplier Onboarding" is open, showing the "Supplier Processing Authority" settings. The modal includes checkboxes for "Authority to Enter", "Authority to Approve", "Authority to Inactivate", and "Supplier Audit". The "Authority to Approve" and "Supplier Audit" options are checked. The modal also has "OK", "Cancel", and "Refresh" buttons.

ORACLE

All Search >> Advanced Search Last Search Results

User Preferences Procurement

User: BSTANLEY Brian Stanley

Location: MAIN MAIN

Origin: ONL Online entry

Department: 0000000 All Departments

Ship To Location: RECEIVING Receiving

Requester: BSTANLEY Stanley, Brian

Buyer:

Contract Process Payables Online Vouchering Purchase Order Authorizations

Rebate Authorizations Receiver / RTV Setup Supplier Processing Authority

Request for Quote Process Requisition Authorizations Doc Tolerance Authorizations

Save Return to Search Previous in List Next in List Notify Refresh

User Preferences | Procurement

Supplier Onboarding

Supplier Processing Authority

User: BSTANLEY Brian Stanley

Supplier Processing Authority

☐ Authority to Enter

☒ Authority to Approve

☐ Authority to Inactivate

☒ Supplier Audit

OK Cancel Refresh

BOR_PORTAL_PERMISSIONS QUERY

Oracle Query Manager interface showing the BOR_PORTAL_PERMISSIONS query.

Query Name: BOR_PORTAL_PERMISSIONS
Description: Portal permissions
Working on selection: Top Level of Query

View field properties, or use field as criteria in query statement.

Col	Record.FieldName	Format	Ord	XLAT	Agg	Heading Text	Add Criteria	Edit	Delete
1	A.ROLENAME - Role Name	Char30				Role Name		Edit	
2	D.PORTAL_OBJNAME - Portal Object Name	Char30				PortlObjNm		Edit	
3	E.PORTAL_LABEL - Portal Label	Char30				PortlLabel		Edit	
4	B.MENUNAME - Menu Name	Char30	1			Menu Name		Edit	
5	B.BARNAME - Menu Bar Name	Char30				Bar Name		Edit	
6	B.BARITEMNAME - Bar Item Name	Char30				Bar Item		Edit	
7	B.PNLITEMNAME - Panel Item Name	Char30				Panel Item		Edit	
8	C.PNLGRPNAME - Component Name	Char18				Component		Edit	

Buttons: Save, Save As, New Query, Preferences, Properties, Publish as Feed, New Union, Return To Search

BOR_PORTAL_PERMISSIONS

Role Name: BOR_PO_VENDORS_APPROVE

OK Cancel

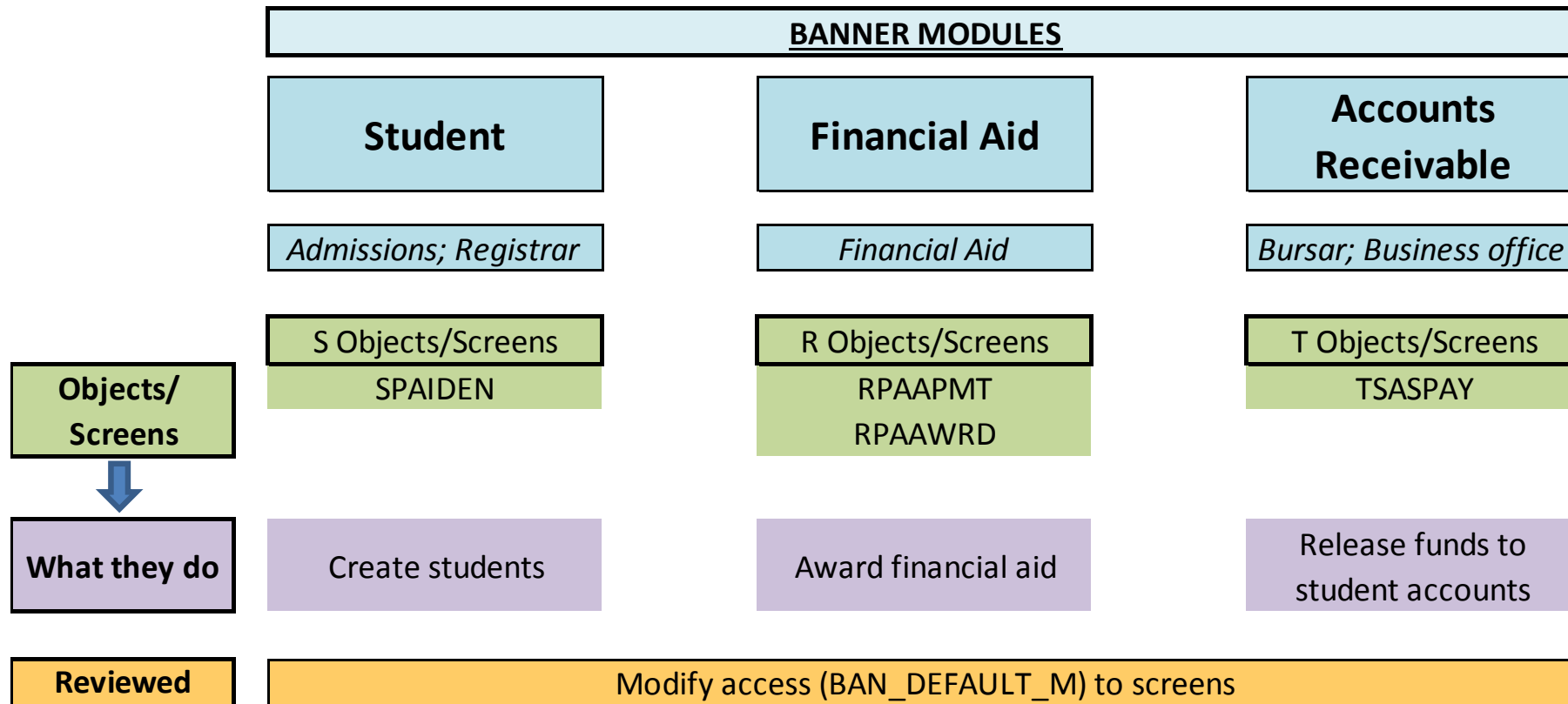
BOR_PORTAL_PERMISSIONS QUERY

This query can be used to see what pages a specific role has access to. So even though this role has Page access to Vendors, doesn't mean that the user can enter or approve. They must have the user preference in addition to the role.

Records	Query	Expressions	Prompts	Fields	Criteria	Having	View SQL	Run
Role Name = BOR_PO_VENDORS_APPROVE								
View All Rerun Query Download to Excel Download to XML			First 1-20 of 20 Last					
	Role Name	PortlObjNm	PortlLabel	Menu Name	Bar Name	Bar Item	Panel Item	Component
1	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_ID1_SUM	APPROVE_VENDOR
2	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	HIDDEN_WORK_PANEL	APPROVE_VENDOR
3	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_DEFL_MASTER	APPROVE_VENDOR
4	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_CUSTOM	APPROVE_VENDOR
5	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_CNTCT	APPROVE_VENDOR
6	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_ADDRESS	APPROVE_VENDOR
7	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	NEW_1099	APPROVE_VENDOR
8	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	LOCATION	APPROVE_VENDOR
9	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	IDENTIFYING_INFORMATION	APPROVE_VENDOR
10	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	HIDDEN_WORK_PANEL	APPROVE_VENDOR
11	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_ID1_SUM	APPROVE_VENDOR
12	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_FEDERAL	APPROVE_VENDOR
13	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_DEFL_MASTER	APPROVE_VENDOR
14	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_CUSTOM	APPROVE_VENDOR
15	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_CNTCT	APPROVE_VENDOR
16	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_ADDRESS	APPROVE_VENDOR
17	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	NEW_1099	APPROVE_VENDOR
18	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	LOCATION	APPROVE_VENDOR
19	BOR_PO_VENDORS_APPROVE	EP_PV_VNDR_APP	Supplier Approval	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	IDENTIFYING_INFORMATION	APPROVE_VENDOR
20	BOR_PO_VENDORS_APPROVE	EP_APPROVE_VENDOR_GBL	Approve Supplier	MAINTAIN_VENDORS	PROCESS	VENDOR_APPROVAL	VNDR_FEDERAL	APPROVE_VENDOR

Banner:

Ineffective Logical Access Controls



Ineffective Logical Access Controls

Modify Access to:	Means:	Implication:
S screens R screens T screens	Someone can add students, award financial aid, and release funds to student accounts.	SOD issue likely
S screens R screens	Someone can add students and award financial aid.	SOD issue likely
R screens T screens	Someone can award financial aid and release to student accounts.	SOD issue likely
S screens T screens	Someone can add students and release funds to their accounts.	SOD not likely

Logical Access Controls

How to review your institution's access in Banner:

- User access for all object class roles in Banner
 - Utilize the Auditing Tool Kit - Script - Class Security Report by Object
- Script must be executed by Banner DBA or Security Admin and run for all objects

Class Security Report by Object				
zaqsc1s.sql				
Date: March 31, 2015 @ 4:44 p.m.				
USER	OBJECTS	CLASS	ROLE	ACTIVITY DATE
MGOOCH	STVWSCF	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	STWSCT	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	STWSFD	BAN_CONSULTING_C	BAN_DEFAULT_M	03-FEB-2014
	STWSPF	BAN_CONSULTING_C	BAN_DEFAULT_M	22-JAN-2015
	STWSPG	BAN_CONSULTING_C	BAN_DEFAULT_M	03-FEB-2014
	STWSSO	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	STVWTHD	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	STVXLBL	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	SUAMAIL	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	SURDELT	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	SURLOAD	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	SZRCAPP	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	TFAACCT	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	TFAANSD	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005
	TFAANSD	BAN_CONSULTING_C	BAN_DEFAULT_M	12-AUG-2005

Logical Access Controls

How to review your institution's access in Banner:

- Listing of Active Employees (Compare to Class Security Report by Object)
- Isolate Critical Objects: SPAIDEN, RPAAPMT, RPAAWRD, and TSASPAY with BAN_DEFAULT_M Role
- Identify conflicting roles
- Review employee's job descriptions
- Discuss mitigating controls

Logical Access Controls

How to review your institution's access in Banner:

- Determine policies or procedures for authorizing users for Banner
- Are adequate measures in place to ensure that when a user is terminated or transferred their access is changed accordingly?
- How long do you retain authorization forms? Does it seem adequate?
- Is access to SFAREGF form limited?
- Verify access to resources and utilities with Banner application is limited
 - Resources – FAFSA – Financial Aid Data Downloads
 - Utilities – Crystal Reports, SQL

Additional Things to Consider

- Document Analysis/Review of Segregation of Duties
- Updated/clear Policies and Procedures for SFA
- Documented - SFA Risk Assessment
- Available documentation – audit evidence
- Banner – Change Management
- All audits and Full Disclosure Management Reports Engagements will receive SFA Compliance for FY 2015. Additionally, those with a federal finding in FY 2014 or previously unresolved SFA findings will be reviewed.

Fort Valley, Clayton, GRU, Ga Southern, GPC, GSU, KSU, VSU, Albany, Columbus, Georgia Southwestern, UNG, SSU, ABAC, Bainbridge, Darton, GGC, East Ga, Gordon, Middle Ga and South Ga