BANNER SECURITY:
AUDITING USER ACCESS

Objectives

Review basic terminology used when reviewing
Banner Security

Review audit techniques for reviewing and
assessing user access and privileges

Provide insight for assessing the adequacy of
segregation of duties

What to audit?

Oracle database
Internet Native Banner
Banner Self-Service
System IDs access
3rd Party Interfaces
IS Analysts/DBA Access
Banner Security

Security maintenance is performed through GSASECR using BANSECR

BANSECR is the security role and should be restricted to DBAs

Banner Objects

Forms
- Input
- Inquiry
Processes (i.e., jobs)
Reports
Tables
- Base
- Validation

Naming Conventions

1st Position – Identifies the Banner System
- A – Alumni/Development
- G – General Person & Security
- F – Finance
- P – Human Resources/Payroll/Personnel
- N – Position Control
- T – Accounts Receivable
- S – Student
- R – Financial Aid
Naming Conventions

2nd Position – Identifies the Application within the System that is the “owner”
  • Letter definition is dependent upon the System

<table>
<thead>
<tr>
<th>Position</th>
<th>2nd Letter</th>
<th>3rd Letter</th>
<th>4th Letter</th>
<th>5th Letter</th>
<th>6th Letter</th>
<th>7th Letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>A</td>
<td>G</td>
<td>P</td>
<td>B</td>
<td>O</td>
<td>F</td>
</tr>
<tr>
<td>- Admissions</td>
<td>A</td>
<td>G</td>
<td>P</td>
<td>O</td>
<td>F</td>
<td>R</td>
</tr>
<tr>
<td>- Admissions</td>
<td>A</td>
<td>G</td>
<td>P</td>
<td>O</td>
<td>F</td>
<td>R</td>
</tr>
</tbody>
</table>

Naming Conventions

3rd Position – Identifies the Object (i.e., Form, Report, Process, Table, etc)
  • A – Application Form (e.g., data entry)
  • B – Base table
  • P – Process
  • I – Inquiry Form
  • Q – Query Form
  • R – Reports or Rule table
  • V – Validation table (where codes are defined)

Naming Conventions

4th - 7th Positions – Identifies the short description of what the Form, Report, Process or Table is.
  • IDEN – Identification
  • TRNH – Transaction Header
  • TRND – Transaction Detail
  • UCLS – User Classes
  • UOBJ – Objects
  • DIRD – Direct Deposit information
Banner Classes

Defines HOW a user accesses the forms and processes
Allows permissions to be defined once, then assigned to many users
Organizes Banner objects into job responsibilities unique to the organization

Banner Classes

A user with access to two classes containing the same object will ALWAYS be granted the class with the higher role for a given object

One of the highest role privilege is BAN_DEFAULT_M

Banner Roles

Groups of Oracle privileges
Vital to securing Banner
Password protected
Password, also call seed numbers, can be changed by DBAs
Banner Roles

Examples

- BAN_DEFAULT_M – maintenance or modify
- BAN_DEFAULT_Q – query or read-only
- BAN_DEFAULT_CONNECT – database connection only, no access to objects. This is the default role.
- BAN_DEFAULT_NO_ACCESS – role has NO privileges and could be assigned to terminated accounts

Institutions have the flexibility to create unique roles with specific privileges

Banner Roles

Banner delivered roles are recognizable

- BAN_xxxxxx_xxxx
- @ ASU, additional roles were developed for IT use only
  - FINANCE_DEV
  - HR_DEV
  - DBA

WHERE DO YOU START?
Security Tables

GURUCLS
GURUOBJ
GOBEACC

GURUCLS

Provides Classes and the assigned Users
Fields
- GURUCLS_USERID: end user
- GURUCLS_CLASS_CODE: Banner Class
- GURUCLS_ACTIVITY_DATE: last date record was changed
- GURUCLS_USER_ID: who made the changes

GURUOBJ

Provides Classes and the assigned Objects
Fields
- GURUOBJ_OBJECT: Banner form, table, report, etc.
- GURUOBJ_ROLE: Privileges assigned
- GURUCLS_USERID: end user or Class
- GURUOBJ_ACTIVITY_DATE: last date record was changed
- GURUOBJ_USER_ID: who made the change
GOBEACC

Matches end users to and Oracle IDs

Fields
- GOBEACC_PIDM: end user unique identifier
- GOBEACC_USERNAME: Oracle ID used to access Banner

WHERE DO YOU RESTRICT ACCESS?

Forms to Review

Finance
- FGBTRND/FGBTRND
- FTMVEND/FTVVEND
- FPARREQN
- FPARDEL
- FPAAGRD
- FPAPURR
- FPARCVD

HR/Payroll/Personnel
- PEAEMPL/PEEMPL
- PEAHIRE
- PEAESCH
- PEA1PAY
- NBAJOBS/NBRJOBS
- PHPCALC
- PHRDOCM/GXADIRD
### Forms to Review

<table>
<thead>
<tr>
<th>Student</th>
<th>Financial Aid</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBRACCD</td>
<td>RFRMGMT</td>
</tr>
<tr>
<td>SPAIDEN/SPRIDEN</td>
<td>RBRCOMP</td>
</tr>
<tr>
<td>SHAINST</td>
<td>RPRGFND</td>
</tr>
<tr>
<td>SHACRSE</td>
<td>RORRULE</td>
</tr>
</tbody>
</table>

## OUR APPROACH TO AUDITING ACCESS

### Auditing Access

To get the full picture, we reviewed:
- what the Classes give Users the ability to do,
- what Users are assigned to the Class, and
- what Objects Users have direct access to.
Auditing Access

1. Select Classes to Audit
2. Obtain a List of Objects for each Class
3. Join the List of Objects to the Objects Spreadsheet using IDEA
4. Review Objects within each Class
5. Obtain a List of Users for each Class
6. Review Users assigned to each Class
7. Obtain a List of Objects Users have Direct Access to
8. Review the Objects Users have Direct Access

Select Classes to Audit

ASU has 158 classes with 519 active users.

Fraud Risk Assessment

- Procurement Process
- Employee Reimbursement Process
- Payroll Process

Auditing Access

1. Select Classes to Audit
2. **Obtain a List of Objects for each Class**
3. Join the List of Objects to the Objects Spreadsheet using IDEA
4. Review Objects within each Class
5. Obtain a List of Users for each Class
6. Review Users assigned to each Class
7. Obtain a List of Objects Users have Direct Access to
8. Review the Objects Users have Direct Access
List of Objects for each Class

BANSEC.GURUOBJ

<table>
<thead>
<tr>
<th>GURUOBJ_OBJECT</th>
<th>GURUOBJ_ROLE</th>
<th>GURUOBJ_USER</th>
<th>GURUOBJ_ACTIVITY_DATE_TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOCOFP</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFP</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFR</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFO</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFF</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFR</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFF</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFP</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FOCOFT</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FODCDS</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FODCDS</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FODCDS</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
<tr>
<td>FODCDS</td>
<td>BAN DEFAULT M</td>
<td>ANS FIN AP</td>
<td>01/2/2005 21:36:22</td>
</tr>
</tbody>
</table>

Object Spreadsheet

<table>
<thead>
<tr>
<th>FORMS</th>
<th>DESCRIPTION</th>
<th>DEFINITION</th>
<th>ADD INFO</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTPACTL</td>
<td>Control Account Maintenance Form</td>
<td>Enables you to create and maintain revenue, expense, and reconciliation accounts in Finance.</td>
<td>CHART OF ACCOUNTS SYSTEM CONTROL MENU</td>
</tr>
<tr>
<td>FTPMGR</td>
<td>Financial Manager Maintenance Form</td>
<td>Enables you to view demographic data about each financial manager and to establish budgetary responsibility for grants, funds, and organizations.</td>
<td>CHART OF ACCOUNTS SYSTEM CONTROL MENU</td>
</tr>
<tr>
<td>FTPMVY</td>
<td>Fiscal Year Maintenance Form</td>
<td>Enables you to establish fiscal year accounting periods.</td>
<td>CHART OF ACCOUNTS SYSTEM CONTROL MENU</td>
</tr>
<tr>
<td>FTPHRD</td>
<td>Hierarchical Budget Maintenance Form</td>
<td>Enables you to establish hierarchical budgetary relationships for the organization within your facility.</td>
<td>CHART OF ACCOUNTS SYSTEM CONTROL MENU</td>
</tr>
</tbody>
</table>

Auditing Access

1. Select Classes to Audit
2. Obtain a List of Objects for each Class
3. Join the List of Objects to the Objects Spreadsheet using IDEA
4. Review Objects within each Class
5. Obtain a List of Users for each Class
6. Review Users assigned to each Class
7. Obtain a List of Objects Users have Direct Access to
8. Review the Objects Users have Direct Access to
Result of the Join

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>ROLE</th>
<th>FORM</th>
<th>DESCRIPTION</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAAMNO</td>
<td>BAA_DEFAULT</td>
<td>FAAMNO</td>
<td>Invoice Credit Memo Cancel Form</td>
<td>Enables you to cancel an invoice that you have completed, approved, and posted.</td>
</tr>
<tr>
<td>FAAMVO</td>
<td>BAA_DEFAULT</td>
<td>FAAMVO</td>
<td>Invoice Credit Memo Form</td>
<td>Enables you to create invoice documents. This form accommodates Direct invoice transactions (invoices that do not involve a purchase order), Regular invoice transactions (invoices that involve a purchase order), and General transaction invoiced transactions (invoices that liquidate a General Accounting Encumbrance).</td>
</tr>
<tr>
<td>FAAMVC</td>
<td>BAA_DEFAULT</td>
<td>FAAMVC</td>
<td>Payment Control Form</td>
<td>Enables you to modify payment due dates and assign or remove funds on completed invoice documents.</td>
</tr>
</tbody>
</table>

Auditing Access

1. Select Classes to Audit
2. Obtain a List of Objects for each Class
3. Join the List of Objects to the Objects Spreadsheet using IDEA
4. **Review Objects within each Class**
5. Obtain a List of Users for each Class
6. Review Users assigned to each Class
7. Obtain a List of Objects Users have Direct Access to
8. Review the Objects Users have Direct Access

Review of Objects within each Class

Segregation of Duties

Unnecessary Access
- Sensitive Data
- Not related to Employee’s Job Function
### Auditing Access

1. Select Classes to Audit  
2. Obtain a List of Objects for each Class  
3. Join the List of Objects to the Objects Spreadsheet using IDEA  
4. Review Objects within each Class  
5. **Obtain a List of Users for each Class**  
6. Review Users assigned to each Class  
7. Obtain a List of Objects Users have Direct Access to  
8. Review the Objects Users have Direct Access

### List of Users for each Class

**BANSEC Website**

**Security Tables**

### Auditing Access

1. Select Classes to Audit  
2. Obtain a List of Objects for each Class  
3. Join the List of Objects to the Objects Spreadsheet using IDEA  
4. Review Objects within each Class  
5. Obtain a List of Users for each Class  
6. **Review Users assigned to each Class**  
7. Obtain a List of Objects Users have Direct Access to  
8. Review the Objects Users have Direct Access
Review of Users in Each Class

Segregation of Duties

Unnecessary Access
- Not related to Employee’s Job Function

Terminated Employees

Auditing Access

1. Select Classes to Audit
2. Obtain a List of Objects for each Class
3. Join the List of Objects to the Objects Spreadsheet using IDEA
4. Review Objects within each Class
5. Obtain a List of Users for each Class
6. Review Users assigned to each Class
7. **Obtain a List of Objects Users have Direct Access to**
8. Review the Objects Users have Direct Access

List of Objects Users have Direct Access

<table>
<thead>
<tr>
<th>BANSEC.R.GURUOBJ</th>
<th>GURUOBJ.DIRECT</th>
<th>GURUOBJ.DATE</th>
<th>GURUOBJ.p</th>
<th>GURUOBJ_ACTIVITY</th>
<th>GURUOBJ_ACTIVITY_DATE</th>
<th>GURUOBJ_ACTIVITY_DATE.TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAWADA</td>
<td>BAN_DEFAULT.D</td>
<td>12/19/2008</td>
<td>12:39:59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRIDIA</td>
<td>BAN_DEFAULT.D</td>
<td>5/19/2008</td>
<td>12:39:59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRIEDIVA</td>
<td>BAN_DEFAULT.D</td>
<td>5/19/2008</td>
<td>12:39:59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GARRIT</td>
<td>BAN_DEFAULT.D</td>
<td>5/19/2008</td>
<td>12:39:59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GARRITO</td>
<td>BAN_DEFAULT.D</td>
<td>6/5/2009</td>
<td>15:15:46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GARRITIT</td>
<td>BAN_DEFAULT.D</td>
<td>6/5/2009</td>
<td>15:15:46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GARRITI</td>
<td>BAN_DEFAULT.D</td>
<td>6/5/2009</td>
<td>15:15:46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PURKADO</td>
<td>BAN_DEFAULT.D</td>
<td>10/26/2006</td>
<td>8:52:20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PURIACI</td>
<td>BAN_DEFAULT.D</td>
<td>10/26/2006</td>
<td>8:52:47</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Auditing Access

1. Select Classes to Audit
2. Obtain a List of Objects for each Class
3. Join the List of Objects to the Objects Spreadsheet using IDEA
4. Review Objects within each Class
5. Obtain a List of Users for each Class
6. Review Users assigned to each Class
7. Obtain a List of Objects Users have Direct Access to
8. Review the Objects Users have Direct Access

Review of Direct Access

Unnecessary Access
• Not related to Employee’s Job Function

Terminated Employees

Controls

Data custodian’s approval of access
Data custodian periodic review
Audit tables
Logging/monitoring of IS Analysts & DBAs
QUESTIONS

Contact Information

Emily A Knopp
emily.knopp@angelo.edu
325-943-2261

Amanda Clark
amanda.clark@ttu.edu
806-743-1050, ext 5