BANNER SECURITY: AUDITING USER ACCESS

EMILY A KNOPP
2011 TACUA CONFERENCE
APRIL 6, 2011

Objectives

Understand the complexities of securing Banner and the related data

Review basic terminology used when reviewing Banner access

Review audit techniques for reviewing and assessing user access and privileges

Apply general audit techniques to assess users' access and the adequacy of segregation of duties

Resources

Banner 8.x General Security Handbook

Banner Objects Description Aid

Technical Teams

What to audit?

- Oracle database
  - User Access
  - DBA/Programmer Access
- Internet Native Banner
  - User Access
  - Approval Queues
- Self-Service Banner
- 3rd Party Interfaces

BANNER BASICS

Banner Security

Security maintenance is performed through GSASECR using BANSECR

BANSECR is the security role and should be restricted to DBAs

BANSECR role can be renamed to create accountability

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*

Finance	HR/Payroll/Position Ctrl	Student	Financial Aid
A – AP	A – Application	A – Admissions	C – Records Creation
G – General Ledger		G – General Student	H – History & transcripts
P – Purch/Proc	P – General Person	P – Person	P – Packaging & Distribution
B – Budget Dev	B – Budget		S – Student Sys Shared Data
O – Operations	O – Overall	O – Overall	
F – Fixed Assets		F – Reg/Fee Assessment	
R – Research Acctng	R – Electronic Approval	R – Recruiting	
S – Stores Inventory	S – Security	S – Scheduling	

Naming Conventions

3rd Position – Identifies the Object (e.g., *Form, Report, Process, Table, etc)*

- A – Application Form (e.g., data entry)
- B – Base table
- P – Process
- I – Inquiry Form
- Q – Query Form
- M – Maintenance 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

Banner delivered classes are application specific

Contains all objects of the application

Default role for objects is BAN_DEFAULT_M

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

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*
- @ TTUS, additional roles were developed for ODBC access
  - *USR_DEFAULT_CONNECT*
  - *USR_SATURN_Q*
  - *USR_POSCTL_Q*
  - *USR_FIMSMGR_Q*

WHERE DO YOU START?

Research

Banner Security Handbook

Security Plan & Approach

Authentication

Active Directory Services

Oracle PIN

IP Address

Security Tables

GURUCLS

GURUOBJ

GURUTAB

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 change

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 Users to Oracle IDs

Fields

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

JOIN to SPRIDEN to identify name of User

WHERE DO YOU RESTRICT ACCESS?

Forms to Review

Finance

- FGBTRND/FGBTRNH
- FTMVEND/FTVVEND
- FPAREQN
- FPARDEL
- FPAAGRD
- FPAPURR
- FPARCVD

HR/Payroll/Personnel

- PEAEMPL/PEBEMPL
- PEAHIRE
- PEAESCH
- PEA1PAY
- NBAJOBS/NBRJOBS
- PHPCALC
- PHRDOCM
- GXADIRD/GXRDIRD

Forms to Review

Student

- TBRACCD
- SPAIDEN/SPRIDEN
- SHAINST
- SHACRSE
- SHATCKN/SHRTCKN

Financial Aid

- RFRMGMT
- RBRCOMP
- RPRGFND
- RORRULE

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 approximately 160 classes

TTUS has approximately 400 classes

Fraud Risk Assessment

- *Procurement Process*
- *Employee Reimbursement Process*
- *Payroll Process*

•Data Risk Assessment

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

BANSECR.GURUOBJ

GURUOBJ_OBJECT	GURUOBJ_ROLE	GURUOBJ_USERID	GURUOBJ_ACTIVITY_DATE_DATE	GURUOBJ_ACTIVITY_DATE_TIME
FOICOMM	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FOICOMP	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FOIDOCH	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FOIIDEN	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FOIVEND	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FOQADDR	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FOQSDLF	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FOQSDLV	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FPAEOCD	BAN_DEFAULT_Q	ASU_FIN_AP	8/12/2005	21:36:31
FPARRIM	BAN_DEFAULT_Q	ASU_FIN_AP	8/12/2005	21:36:31
FPIEOCL	BAN_DEFAULT_Q	ASU_FIN_AP	8/12/2005	21:36:31
FPIIREC	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31
FPIOPOF	BAN_DEFAULT_M	ASU_FIN_AP	8/12/2005	21:36:31

Object Spreadsheet

FORMS	DESCRIPTION	DEFINITION	Add. Info
FTMACTL	Control Account Maintenance Form	Enables you to create and maintain revenue, expense, transfer, and encumbrance control accounts in Finance.	CHART OF ACCOUNTS SYSTEM CONTROL MENU
FTMFMGR	Financial Manager Maintenance Form	Enables you to view demographic data about each financial manager and to establish budgetary responsibility for grants, funds, and organizations.	CHART OF ACCOUNTS SYSTEM CONTROL MENU
FTMFSYR	Fiscal Year Maintenance Form	Enables you to establish fiscal year accounting periods.	CHART OF ACCOUNTS SYSTEM CONTROL MENU
FTMHBUD	Hierarchical Budget Maintenance Form	Enables you to establish hierarchical budgetary relationships for the organizations within your facility.	CHART OF ACCOUNTS SYSTEM CONTROL MENU

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

Result of the Join

OBJECTS	ROLE	FORM	DESCRIPTION	DEFINITION	ADD_INFO
FAAINVD	BAN_DEFAULT_M	FAAINVD	Invoice/Credit Memo Cancel Form	Enables you to cancel an invoice that you have completed, approved, and posted.	INVOICE/CREDIT MEMO PROCESSING MENU
FAAINVE	BAN_DEFAULT_M	FAAINVE	Invoice/Credit Memo Form	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 Encumbrance invoice transactions (invoices that liquidate a General Accounting Encumbrance).	INVOICE/CREDIT MEMO PROCESSING MENU
FAAPAYC	BAN_DEFAULT_M	FAAPAYC	Payment Control Form	Enables you to modify payment due dates and assign or remove holds on completed invoice documents.	INVOICE/CREDIT MEMO PROCESSING MENU

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

BANSECR.GURUOBJ

GURUOBJ_OBJECT	GURUOBJ_ROLE	GURUOBJ_USERID	GURUOBJ_ACTIVITY_DATE_DATE	GURUOBJ_ACTIVITY_DATE_TIME
SAAADMS	BAN_DEFAULT_Q	AAGUILAR9	12/19/2008	12:35:26
RPRLNDA	BAN_DEFAULT_M	AAGUILAR9	5/19/2008	8:40:13
RPRLNDR	BAN_DEFAULT_M	AAGUILAR9	5/19/2008	8:40:13
SFASTCA	BAN_DEFAULT_Q	AAGUILAR9	5/19/2008	8:40:13
GEAATID	BAN_DEFAULT_M	AASHCRAFT	6/17/2009	15:15:46
GEIATTD	BAN_DEFAULT_M	AASHCRAFT	6/17/2009	15:15:46
GTVSDAX	BAN_DEFAULT_M	ABALCH	6/21/2006	9:33:32
PEAFACD	BAN_DEFAULT_Q	ABALCH	10/26/2006	8:52:39
PEAFACT	BAN_DEFAULT_Q	ABALCH	10/26/2006	8:52:47

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

Internal Controls

Approval and removal process for access

Periodic review of

- Users to Classes
- Objects to Classes
- Direct Grants

Internal Controls

Audit tables

Logging/monitoring of IS Analysts & DBAs

QUESTIONS
???

Contact Information

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