How the U.S. Department of the Interior (DOI) Successfully Implemented SAP BusinessObjects Access Control

Martin Kessler, U.S. DOI • Sonny Dasgupta, SAP
## Learning Points

- In this session, we will answer the following questions:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why AC?</td>
<td>The capabilities of SAP Access Control</td>
</tr>
<tr>
<td>Why?</td>
<td>Business goals for automating manual security processes by implementing FBMS Access Control</td>
</tr>
<tr>
<td>What?</td>
<td>The FBMS Access Control solution</td>
</tr>
<tr>
<td>How?</td>
<td>Factors key to the success of FBMS Access Control</td>
</tr>
<tr>
<td>So What?</td>
<td>The value of the FBMS Access Control solution</td>
</tr>
</tbody>
</table>

Real Experience. Real Advantage. 2
What We’ll Cover …

- Introduction to SAP Access Control
- Overview of the Department of the Interior and the FBMS Program
- Business Goals for the FBMS Access Control Implementation
- The FBMS Access Control Solution
- Key Success Factors
- The Value of the FBMS Access Control Solution
- Wrap-up
SAP BUSINESSOBJECTS

Access Control

Today's Issues

- FRAGMENTED
- LACK OF COLLABORATION
- MANUAL PROCESSES → ACCESS RISK ↑
- MANUAL SOD PROCESSES → SOD CONFLICTS ↑
- AUDIT ↑

RISK ANALYSIS

SUPER USER MANAGEMENT

USER PROVISIONING

Role Design

EASY ENFORCEMENT

NAY

REAL TIME.

Results

- ENTERPRISE WIDE
- AUTOMATED E2E (ARM)
- IT BY BUSINESS
  COLLABORATE

AUTOMATE

Access Risk ↓

AUTOMATE SOD
SOD Conflicts ↓

PREVENT FRAUD

REDUCE AUDIT
SAP Access Approver mobile app

✔ Standardized, simplified provisioning process

- Display lists of user and firefighter access requests
- Review user and firefighter access requests, with access details
- Review risks associated with a request (if risk analysis has already been performed)
- Call or email users to request additional information
- Add comments before approving or rejecting requests
- Forward requests to people in your Contacts list in cases when further analysis and simulation is needed
What We’ll Cover …

- Introduction to SAP Access Control
- Overview of the Department of the Interior and the FBMS Program
- Business Goals for the FBMS Access Control Implementation
- The FBMS Access Control Solution
- Key Success Factors
- The Value of the FBMS Access Control Solution
- Wrap-up
U.S. Department of the Interior

- The U.S. Department of the Interior is a Cabinet-level agency that manages America's vast natural and cultural resources.
- The DOI mission is to protect America’s natural resources and heritage, honor our cultures and tribal communities, and supply the energy to power our future.
The Department is organized into the following technical bureaus, as well as 60 Departmental Offices:
The Department:

- Employs nearly 70,500 employees in approximately 2,400 locations across twelve time zones
- Manages more than 500 million, or 1 in every 5, acres of the land area of the United States
- Manages 397 units of the national park system, 556 national wildlife refuges, 71 fish hatcheries and one historic fish hatchery, 21 national conservation areas, and 16 national monuments
- Manages areas that produce approximately 24 percent of the nation’s energy
FBMS Vision

“FBMS is the cornerstone of a fully integrated business management system, supporting DOI as a world-class organization acknowledged for management excellence and effective mission delivery.”

FBMS Executive Steering Committee
Overview of FBMS

- Functional footprint of FBMS: Finance, Acquisition, Financial Assistance, Personal Property, Fleet, Real Property, and an Enterprise Management Information System (EMIS)
- As of November 2011, seven DOI bureaus, which includes 60 Departmental Offices, have deployed FBMS, accounting for a user community of approximately 8,500 users.
- In November 2012, the FBMS user community is projected to more than double with the deployment of two additional bureaus.
- In November 2013, the final bureau will deploy FBMS, bringing the user community to around 22,000.
FBMS Technical Architecture

Enterprise Management Information System (EMIS) (SAP BW, BusinessObjects)

Document Management & Archiving (OpenText)

Core Financials, Personal Property, Fleet Maintenance, Real Property, and Requisitioning SAP ECC 6.0

Budget Formulation, Consolidated Financials (Deployment TBD)

SAP Enterprise Portal

Enterprise Application Integration (SAP PI)

User Management and Separation of Duties Analysis (SAP GRC v5.3 – Access Control Suite)

Acquisition and Financial Assistance (PRISM v6.5)
What We’ll Cover …

- Introduction to SAP Access Control
- Overview of the Department of the Interior and the FBMS Program
- Business Goals for the FBMS Access Control Implementation
- The FBMS Access Control Solution
- Key Success Factors
- The Value of the FBMS Access Control Solution
- Wrap-up
Security Processes Through FBMS Deployment 5

- Through Deployment 5 (D5) of FBMS, the processes for registering users, adding and removing roles, and deactivating users required a great deal of manual effort by requestors, approvers, and security administrators:
  - 18-page paper-based access request form
  - Manual signatures by Account Controllers (approvers)
  - If Account Controllers were geographically decentralized, the access request form was either faxed or scanned and e-mailed among locations
  - Completed form was attached to a Remedy ticket
  - Security administrators (known as Security Points of Contact or SPOCs) within each bureau manually created users, assigned or removed roles, or deactivated users
Due to the use of Single Sign-On (SSO) for authentication purposes, as well as the overall design of the system, FBMS seems like a single, integrated system to the end user.

However, from a security administration perspective, SPOCs were required to update as many as five different back-end systems for a single role assignment or role removal.

For instance, in order to assign the Acquisitions Contracting Officer (ACQ_CO) role to an end user, a SPOC assigned five separate technical roles to the end user:

- ECC Portal Role
- BW Portal Role
- BW Role
- ECC Role
- PRISM Role
DOI developed a quasi-automated process for providing emergency access to members of the FBMS Production Support team in order to work production issues.

- Paper-based access request form
- Manual signatures by Account Controllers (approvers)
- Access request form was either faxed or scanned and e-mailed between two primary Account Controller locations
- Completed form was attached to a Remedy ticket
- Security administrators unlocked a designated Emergency Privilege (EP) user ID, reset the password, and provided the password to the requestor
- Information Assurance (IA) team reviewed transactions performed by EP users for appropriateness
Business Goals for the FBMS Access Control Implementation

- In light of these manual security processes, and with the footprint of the FBMS user community expanding with each deployment, DOI recognized a major opportunity for improvement through automation—the automated solution is called FBMS Access Control.

- The primary business goals for the implementation of FBMS Access Control were to:
  - Streamline security processes and improve efficiency and FBMS user productivity through automation
  - Enhance the user experience for requestors, SPOCs, and Account Controllers
  - Reduce requestor, SPOC, and Account Controller workload
  - Improve compliance with federal government and departmental security policies (A-123, FISMA, DOI IT Security Policy)
What We’ll Cover …

- Introduction to SAP Access Control
- Overview of the Department of the Interior and the FBMS Program
- Business Goals for the FBMS Access Control Implementation
- The FBMS Access Control Solution
- Key Success Factors
- The Value of the FBMS Access Control Solution
- Wrap-up
The FBMS Access Control Solution

- With FBMS Deployment 6, which went live in October 2011, DOI implemented FBMS Access Control. This solution provides an integrated, automated, workflow-based solution for:
  - User Account Management
  - Separation of Duties (SOD) Analysis
  - Emergency Privilege (Firefighter) Processes
FBMS Access Control Workflows

- FBMS Access Control, which is based on the SAP BusinessObjects Access Control suite (version 5.3), includes the following automated workflows:

  Request Access:

  Welcome to the Request Access page
  Help is available for each link; click the link located on the top of this page

  - **Finalize New User Registration:** Requestor - Use this selection to complete the FBMS account registration process
  - **Role Request:** Requestor - Use this selection to add or remove roles
  - **Update User Master Record:** Requestor - Use this selection to update user information, such as Last Name, First Name, FBMS Office Code, FBMS Accounting Number, User Type, PRISM Site ID, PRISM Warrant Information, PRISM Sign in Rights, PRISM Evaluator Only, and PRISM FPDS-NG ID
  - **Remove Access:** Requestor - Use this selection to remove one or more roles from a user account
  - **Deactivate User Account:** Requestor - Use this selection to deactivate a user account
  - **Table Update:** SPOC/Account Controller use only - Use this selection to update the PSS/OAWS tables
  - **EP Request:** FBMS PMO use only - Use this selection to request the use of an Emergency Privilege (EP) ID
The purpose of each FBMS Access Control workflow is summarized below:

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Initiate New User Registration</td>
<td>These two workflows are used in combination to register a new FBMS user</td>
</tr>
<tr>
<td>2) Finalize New User Registration</td>
<td></td>
</tr>
<tr>
<td>3) Role Request</td>
<td>This workflow is used to request new roles for or remove existing roles from an FBMS user</td>
</tr>
</tbody>
</table>
| 4) Update User Master Record    | This workflow is used to make updates to the following fields associated with a FBMS user account:  
                                      • Last Name  
                                      • First Name  
                                      • FBMS Office Code  
                                      • FBMS Accounting Number  
                                      • User Type  
                                      • PRISM Site ID  
                                      • PRISM Sign in Rights  
                                      • PRISM Evaluator Only  
                                      • PRISM FPDS-NG ID  
                                      • PRISM Warrant Information |
The purpose of each FBMS Access Control workflow is summarized below (continued):

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5) Table Update</td>
<td>This workflow is used to make updates to the PSS and OAWS tables in FBMS</td>
</tr>
<tr>
<td>6) Remove Access</td>
<td>This workflow is used to remove all roles from a FBMS user account</td>
</tr>
</tbody>
</table>
| 7) Deactivate User Account| This workflow is used to deactivate a FBMS user account, which includes the following actions:  
  • Locking the user account (if it is not already locked)  
  • Moving the user account to the “Deleted” user group in FBMS  
  • Removing the user account from the PSS and OAWS tables (if applicable)  
  • Deactivating the user account in PRISM  
  • Removing any role check boxes in PRISM |
| 8) Emergency Privilege (EP) Request | This workflow is used to provide emergency access to members of the FBMS Production Support team in a controlled, auditable environment. |
Initiate New User Registration

- Registration for a new FBMS user is a two-step process:
  - Step 1: Initiate New User Registration
    - Custom DOI solution
  - Step 2: Finalize New User Registration
    - Workflow through FBMS Access Control

DOI developed a custom Portal object and ABAP enhancement that work together to automatically generate a unique user ID (based on the FBMS naming convention) and map this ID to the user’s Active Directory ID for SSO purposes. These activities occur without any manual intervention by the DOI SPOCs, thus streamlining the FBMS new user registration process.
Finalize New User Registration Workflow

- The second step in the registration process for a new FBMS user is triggered through the Finalize New User Registration workflow.
Finalize New User Registration Workflow (cont.)

- Within FBMS Access Control, the Finalize New User Registration workflow is initiated by the Requestor (or someone acting on behalf of the Requestor), validated by the SPOC, and approved by the Account Controller.
  - Although each workflow is standardized across all DOI bureaus within FBMS Access Control, each bureau defines its own SPOCs and Account Controllers.

Within the first three months of the initial go-live of FBMS Access Control, 83% of new user registrations were finalized on the same day they were initiated.
The Role Request workflow is used to request new roles for or remove existing roles from an FBMS user.

- **Role Request**: Requestor - Use this selection to add or remove roles
The Role Request workflow is initiated by the Requestor (or someone acting on behalf of the Requestor) (Step 1) and then validated by the SPOC (Step 2).

The roles that are being requested determine the specific Account Controllers who must approve the request at Step 3.

If the Role Request violates FBMS SOD rules, a role must be removed or a mitigating control must be approved by an Internal Controls Coordinator (Step 4).

The Training Coordinator confirms that all required role-based training has been completed by the user and/or schedules the required training in the DOI Learning Management System (Steps 5 and 6).

After all required training has been completed, the SPOC validates the role request (Step 7) and the roles are automatically provisioned in FBMS (Step 8).
Role Request Workflow (cont.)

- The Role Request workflow presented DOI with a number of challenges.
- Role Request Challenge #1
  - In the legacy FBMS access request process, a user’s Manager was one of the approvers who would sign the hard copy access request form.
  - Many Managers within DOI are not FBMS users, so DOI was faced with the challenge of designing a solution that did not unnecessarily increase the number of FBMS users solely for the purpose of approving access requests.

In order to retain the active participation of Managers in the FBMS access request process without unnecessarily increasing the number of FBMS users, Managers receive system-generated emails from the FBMS Access Control system that notifies them when access requests are initiated for their staff. It is the responsibility of each Manager to notify their bureau SPOCs if they do not agree with a specific role that is being requested and/or they are not the correct Manager for the user who is requesting access to FBMS.
Role Request Challenge #2

As the technical footprint of FBMS is comprised of both SAP and non-SAP systems, it was required that the FBMS Access Control solution be able to perform automated user provisioning and SOD analyses within all FBMS systems.

In order to meet this requirement, DOI engaged a third-party company to build two custom interfaces between PRISM and the CUP and RAR modules of FBMS Access Control.
Role Request Challenge #3

In order to fully realize the benefits of the automation provided by FBMS Access Control, it was imperative that the end user be able to request a single business role (for instance, the ACQ_CO role) as opposed to requesting the five separate technical roles (ECC Portal role, BW Portal role, ECC role, BW role, and PRISM role) required to perform the functions of an Acquisitions Contracting Officer.
Role Request Workflow (cont.)

- Role Request Challenge #3 (continued)
  - In order to meet this requirement, DOI leveraged the role mapping functionality available in version 5.3 of SAP BusinessObjects Access Control. Within FBMS Access Control, end users are able to request a single business role (ACQ_CO) and will automatically be assigned all five corresponding technical roles as part of the automated provisioning (Step 8 of the Role Request workflow).

By leveraging the role mapping functionality available in version 5.3 of SAP BusinessObjects Access Control, the technical roles that comprise a single business role are provisioned instantaneously after all approvals are received within FBMS Access Control. In the legacy process, SPOCs would spend an average of 30 minutes per request assigning up to as many as five corresponding technical roles to fulfill the request of a single business role.
The Table Update workflow is used to make updates to the PSS and OAWS tables in FBMS. These two tables are integral to specific Accounts Payable business process functionality.

**Request Access:**

Welcome to the Request Access page.
Help is available for each link; click the link located on the top of this page.

- **Finalize New User Registration:** Requestor - Use this selection to complete the FBMS account registration process.
- **Role Request:** Requestor - Use this selection to add or remove roles.
- **Update User Master Record:** Requestor - Use this selection to update user information, such as Last Name, First Name, FBMS Office Code, FBMS Accounting Number, User Type, PRISM Site ID, PRISM Warrant Information, PRISM Sign in Rights, PRISM Evaluator Only, and PRISM FPDS-NG ID.
- **Remove Access:** Requestor - Use this selection to remove one or more roles from a user account.
- **Deactivate User Account:** Requestor - Use this selection to deactivate a user account.
- **Table Update:** SPOC/Account Controller use only - Use this selection to update the PSS/OAWS tables.
- **EP Request:** FBMS FMO use only - Use this selection to request the use of an Emergency Privilege (EP) ID.
Table Update Workflow (cont.)

- Within FBMS Access Control, the Table Update workflow is initiated by the Requestor (or someone acting on behalf of the Requestor), validated by the SPOC, and approved by the Account Controller.
- Each DOI bureau designated a small number of Accounts Payable Subject Matter Experts (SMEs) to serve as the Account Controller (approver) in this workflow.

In order to facilitate automated updates to the PSS and OAWS tables in FBMS, DOI engaged a third-party company to build a custom interface between the CUP module of FBMS Access Control and the back-end ECC system.
What We’ll Cover …

- Introduction to SAP Access Control
- Overview of the Department of the Interior and the FBMS Program
- Business Goals for the FBMS Access Control Implementation
- The FBMS Access Control Solution
- Key Success Factors
- The Value of the FBMS Access Control Solution
- Wrap-up
What were some of the success factors that helped DOI traverse the canyon between manual security processes and FBMS Access Control?
FBMS Access Control Key Success Factors (cont.)

- “Tone at the top”
  - Buy-in from senior management
- “Begin with the end in mind”
  - Common understanding of business goals and appreciation for the potential value of the FBMS Access Control solution
  - Federal acquisition lead-time for both software and services were taken into consideration when developing overall project plan
- One size must fit all
  - Bureau buy-in of security process standardization
- Plain, old-fashioned teamwork
  - Integrated project plan and collaboration among FBMS workstreams (Security, Information Assurance, Basis, Portal, Application Development, and Business Process teams)
“Best of both worlds”
- Ideas and insights were provided by both previously deployed DOI bureaus (who had experience with the old, manual security processes) and the newly deploying bureaus (who had never taken part in the legacy processes)

“Tell me, show me, let me”
- Training included a balance of instructor taught concepts, live demonstrations, and practice exercises completed by participants

“Variety is the spice of life”
- End user documentation was developed for two different learning styles (in two different levels of detail)
  - Quick Reference Guides provide guidance in 1-2 pages
  - Work Step Instructions provide step by step, screen by screen, button by button guidance for each workflow
FBMS Access Control Key Success Factors (cont.)

- Frequent outreach to bureau stakeholders, including multiple avenues and mechanisms for collecting feedback
  - Bureaus participated in FBMS Access Control solution blueprinting and approved Business Process Design (BPD) document
  - Bureaus attended monthly calls and provided feedback on key configuration or user interface decisions
  - Bureaus attended numerous live demos of the solution that were conducted before and during testing
  - Bureaus executed test cases during both integration and user acceptance testing
  - Bureaus provided detailed feedback on pilot training materials
  - Bureaus attended combination of Instructor Led Training and Knowledge Transfer WebExes related to FBMS Access Control

DOI bureau stakeholders were consulted and provided invaluable feedback on the FBMS Access Control solution during all phases of the implementation.
Key Success Factor Checklist

- The following Key Success Factor Checklist is based on DOI’s Access Control implementation experience. Not all DOI success factors will be relevant to all Access Control implementations.

  #1 – Do you have buy-in from senior management?
  #2 – Do stakeholders have a common understanding of the business goals and an appreciation for the potential value of the solution?
  #3 – Did you take the acquisition lead-time for both software and services into consideration when developing your overall project plan?
  #4 – Have all stakeholders bought into the standardization of the processes that your solution will support?
  #5 – Does your project plan integrate tasks and dependencies among all workstreams?
  #6 – Have you gathered ideas and insights from both stakeholders who had experience with your legacy processes and those who have not been involved in the legacy processes?
  #7 – Does your training include a balance of instructor taught concepts, live demonstrations, and practice exercises?
  #8 – Does your end user documentation include quick reference guides and detailed, step-by-step instructions?
  #9 – Did you involve stakeholders in all phases of the implementation and provide multiple avenues for collecting feedback?
What We’ll Cover …

- Introduction to SAP Access Control
- Overview of the Department of the Interior and the FBMS Program
- Business Goals for the FBMS Access Control Implementation
- The FBMS Access Control Solution
- Key Success Factors
- The Value of the FBMS Access Control Solution
- Wrap-up
The Value of the FBMS Access Control Solution

Three months after going live with FBMS Access Control, DOI took a step back and measured the quantitative and qualitative value of the solution.
Value of FBMS Access Control – New User Registrations

New User Registrations

- 1 Day
- 0.7 Days
- 30% Increased Employee Productivity
- 83% Percent Finalized in < 1 Day

Strategic Benefits
- Streamlined Process
- Eliminated Bottlenecks
- Reduced Security FTE Labor
- Enhanced Support by SPOCs
- Employees Effective and Efficient Sooner

FBMS Access Control triggered a paradigm shift in the responsibilities of DOI security staff. Since user provisioning tasks that were previously performed manually by SPOCs have now been automated, SPOCs are able to spend the majority of their time acting as business analysts (working directly with requestors and approvers to ensure users receive the right level of access) rather than performing manual security administration tasks.
Value of FBMS Access Control – Role Requests

Role Requests

Strategic Benefits

- Streamlined Process
- Eliminated Bottlenecks
- Reduced Security FTE Labor
- Improved Compliance
- Enhanced Support by SPOCs
- Employees Effective and Efficient Sooner

After the access request form was signed by the final approver in the legacy manual process, scanning the form, creating the Remedy ticket, and the manual provisioning tasks performed by the SPOCs would take an average of 1 hour to complete. Upon final approval of the Role Request workflow in FBMS Access Control, the user provisioning in all FBMS systems is instantaneous.
Value of FBMS Access Control – Role Removals

**Role Removals**

- Manual Process: 1 Day +
- FBMS Access Control: 0.5 Day
- Percent Finalized in < 1 Day: 87%

**Strategic Benefits**
- Streamlined Process
- Eliminated Bottlenecks
- Reduced Security FTE Labor
- Reduced Risk and Better Audit Results
Value of FBMS Access Control – EP Requests

- The automation of Emergency Privilege processes at DOI has resulted in many benefits to the Department:
  - Within the first two weeks of implementing the automated EP process, the average time to request, approve, and provision an EP session was only 1.5 hours.
  - The Security team is no longer involved in the EP process except for off-hours requests and general error resolution.
  - The process is simpler for Production Support staff since they now perform EP transactions with their own user ID rather than a separate EP ID.
  - FBMS Access Control streamlined the Information Assurance team’s review of activities performed by EP users.
  - All of these benefits result in an enhanced level of production support to the FBMS user community.
What We’ll Cover …

- Introduction to SAP Access Control
- Overview of the Department of the Interior and the FBMS Program
- Business Goals for the FBMS Access Control Implementation
- The FBMS Access Control Solution
- Key Success Factors
- The Value of the FBMS Access Control Solution
- Wrap-up
Key Learnings and Best Practices

- Build a business case and gain senior management buy-in.
- Ensure that stakeholders have a common understanding of the business goals and an appreciation for the potential value of the solution.
- Understand the software’s capabilities and limitations and identify any technical challenges during initial project planning.
- Build a project plan that integrates tasks and dependencies among all workstreams.
- Develop training materials that include a balance of instructor taught concepts, live demonstrations, and practice exercises.
- Involve stakeholders in all phases of the implementation and provide multiple avenues for collecting feedback.
Questions?

How to contact me:
Martin Kessler
Martin_Kessler@fbms.doi.gov
Thank you for participating.

Please remember to complete and return your evaluation form following this session.

For ongoing education on this area of focus, visit the Year-Round Community page at www.asug.com/yc