Discovery Session
User Accounts Provisioning

October 3, 2013
Introductions
## Presentation

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introductions</td>
<td>2</td>
</tr>
<tr>
<td>Agenda</td>
<td>3</td>
</tr>
<tr>
<td>Housekeeping</td>
<td>5</td>
</tr>
<tr>
<td>Workshop Roles</td>
<td>6</td>
</tr>
<tr>
<td>Objectives and Workshops</td>
<td>7</td>
</tr>
<tr>
<td>Control Primer</td>
<td>13</td>
</tr>
<tr>
<td>Current State – Yale Access Provisioning</td>
<td>15</td>
</tr>
<tr>
<td>What We’ve Learned So Far</td>
<td>16</td>
</tr>
<tr>
<td>Current State - Governance</td>
<td>17</td>
</tr>
<tr>
<td>Current State – Compliance and Administration</td>
<td>18</td>
</tr>
<tr>
<td>Closing and Debrief</td>
<td>19</td>
</tr>
<tr>
<td>Action Items</td>
<td>20</td>
</tr>
</tbody>
</table>
✓ **No** Technology

✓ Be Fully Present

✓ We will have one break

✓ Refreshments will be provided

✓ **No** Notes – will have designated note takers
# Workshop Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Name / Area of Responsibility</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Facilitators          | - Karen Rossetti / Security & Controls Lead  
- Richard Rudnicki / Security & Controls Lead                                           | - Conduct and guide workshops  
- Question and challenge workshop participants when appropriate  
- Provide information necessary for discussion |
| Data Collection Owners| - Karen Rossetti / Security & Controls Lead  
- Richard Rudnicki / Security & Controls Lead  
- John DeNezzo / Security & Controls Analyst                                            | - Lead the pre-work prior to the discovery workshop to collect necessary data  
- Be prepared to discuss source material that was collected as part of the discovery workshop discussion |
| Participants          | **Stakeholders**                                                                                | - Read pre-read materials  
- Complete pre-workshop tasks  
- Actively participate in sessions  
- Identify key points of current process and pain points  
- Represent your stakeholder group  
- Address open items promptly |
| Team Leads            | - Karen Rossetti / Security & Controls Lead  
- Richard Rudnicki / Security & Controls Lead                                           | - Oversee daily progress and performance of workshops  
- Actively participate in sessions  
- Communicate matters requiring attention to program management |
| Minutes / Note Takers | **XXXX**                                                                                       | - Document meeting minutes, action items, and key discussion topics  
- Put relevant information into appropriate PMO tool  
- Ensure notes are published to the full audience |
Objectives and Workshops

- Simplify and standardize processes
- Make it easy to get work done and harder to make mistakes

Establish an accurate, trusted and timely reporting environment

Minimize administrative overhead for faculty and end users

Lower operating costs and improve effectiveness

Workday@Yale
Objectives and Workshops (cont.)

Each workshop is scheduled to follow the same overall structure, although timing / duration of each section may vary.

- **Objectives**
  - “Why are we here?”
  - Overall workshop purpose
  - “What are we working towards?”
  - Expected outputs
  - Focus areas
  - “What does that word mean?”
  - Review of any new terms

- **Re-Cap**
  - “What have we done so far?”
  - Overview of previous workshops’ progress and key items

- **Execution**
  - “Let’s get down to business.”
  - Discussion
  - Pain Points
  - Action Items

- **Closing**
  - “What did we get done today?”
  - Re-cap of documentation
  - Review of Action Items

- **Debrief**
  - “How are we doing?”
  - Review of progress
  - Participant feedback
The Workday@Yale program will present Yale with a requirement to focus on maintaining an effective level of existing security and privacy practices. It also provides an opportunity to improve them through a risk based approach that rationalizes security related efforts and associated roles.

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Workshops</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The objectives for the current state workshops are:</td>
<td>• Security and Controls Discovery workshops are scheduled for the following areas:</td>
</tr>
<tr>
<td>• Document current state of Yale security</td>
<td>• Financial Applications</td>
</tr>
<tr>
<td>• Confirm regulatory and compliance requirements impacting security</td>
<td>• HR, Payroll and Faculty Applications</td>
</tr>
<tr>
<td>• Shed light on people, process, and technology impacts along with current pain points associated with security at Yale</td>
<td>• User Accounts Provisioning</td>
</tr>
<tr>
<td>• Lay foundation for future state security for the Workday@Yale program.</td>
<td></td>
</tr>
</tbody>
</table>
Objectives and Workshops (cont.)

You are EMPOWERED to:

- **ASK** open ended and thought provoking questions to inspire deeper thought into current processes, reports and systems

- **REPRESENT** your stakeholder group

- **RESOLVE** relevant open action items prior to and during meetings to further progress of the workshops as a whole

- **COLLABORATE** with representatives from different functional areas as their input will be crucial to a successful overall implementation

- **SPEAK** up! All voices are important and all of you have been specifically requested to attend

- **LISTEN** attentively and empathetically, allowing each team member the right to speak
Inputs received through the Security & Controls discovery sessions will be utilized to plan for, and execute, a focused thread of security and control related activities to support the overall Workday@Yale implementation.
In preparation for this workshop, the Security & Controls team has met with stakeholders, reviewed documentation, and developed a workshop agenda to help gather background on the current state of Yale’s security & controls environment.

### Activities to Date

- Met with for their preliminary input:
  - Chief Information Security Officer (CISO)
  - Research Compliance Officer
  - HIPAA/Privacy Officer
  - Workday Sponsored Awards Team leads
  - IAM Team
- Researched applicable regulations & policies
- Distilled & summarized security & controls related pain points from HCM, Finance, BI/Reporting, and Technology discovery sessions*
- Performed a review & validation of current state "roles" and YAS security configurations within Oracle EBS and DWH

* Activity still in progress

### Topics to be Considered

Topics that should be considered in today’s session:

- Level set on controls
- Review pain point emerging themes
- Identify other “provisioning” pain points related to:
  - Governance
  - Compliance
  - Administration
Yale must be diligent and responsible for safeguarding its assets.

Consistent with the Planning & Financial Management Program (PFM), the Workday@Yale program will need to consider internal controls (including security) to safeguard assets and help meet business objectives.
Controls are required to protect confidential or sensitive information, maintain financial reporting integrity, manage business operations, and comply with regulatory requirements, standards and policies.

Controls can be preventative or detective in nature and be broadly categorized into the following types:

<table>
<thead>
<tr>
<th>Controls Primer (cont)</th>
</tr>
</thead>
</table>
| Access Controls (a.k.a. Security) | » Restrict access to sensitive data and functionality  
» Enforce segregation of duties and facilitate privacy requirements  
» Preventative in nature |
| System Enabled Controls | » Automated controls enabled through system (i.e. edits, workflows, tolerances, matching, etc.)  
» Generally preventative in nature |
| Manual/Monitoring Controls | » Manual (documented) procedures  
» Control / Compliance reporting and event logging / system auditing  
» Generally detective in nature |

Controls should be:
- Risk-based so control efforts are made only when risks associated with processes warrant controls and costs of controls should not outweigh risks being addressed
- Preventative and automated where possible
- Well documented, clearly communicated and monitored to remain effective
Yale Access Provisioning Diagram

Yale Access Provisioning Overview
Current State

Population of YAS Values

User Accounts

EBS Sysadmin
InfoEd - IRES
YAS Wizard
Populate some IRES Values

Population of YAS Values

START
EBS Sysadmin

Xtrain
User-Side Value Population

YAS

YAS DB

EBS Database

YASified Objects

Oracle DWH

YASified Views

Additional Provisioning Steps Include:
1. Creation of user in EBS;
2. Provisioning of START Responsibility;
3...

Access Request for Distributed Functions: Allows Add/Delete/Modify of YAS values; services specific domains: Domains – Access Orgs, Access Projects, Confidential Jobs, Confidential Orgs; other domains do not go through START

For "Add" Functions and Domain Values, START takes users to Xtrain; Some access does not require training, and will be a "pass through" in other cases specific permission from a Process owner may be required and will be workflows for approval eg: Function "View All Balance-Level Financial Information"
### Pain Points – Emerging Themes:

<table>
<thead>
<tr>
<th>Governance</th>
<th>Controls</th>
<th>Security (Access Controls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Select Policies May Not be Clear or Enforced Properly</td>
<td>• Over Reliance on Cumbersome Manual Processes/Workflows</td>
<td>• Security/Data Access Model is Overly Granular and Complicated to Administer</td>
</tr>
<tr>
<td>• Fulfillment of Training is Difficult to Monitor</td>
<td>• Manual Control Procedures Are Often Lacking</td>
<td>• Provisioning is Complicated and Difficult to Administer</td>
</tr>
<tr>
<td>• Lack of Efficient and Effective Security Attestation Tools and Processes</td>
<td>• Specific Training on Controls Is Lacking</td>
<td>• Roles Are Not Standardized, Rationalized and Do Not Utilize Consistent Approaches to Manage Access Within and Across Systems</td>
</tr>
<tr>
<td>• No Overarching Strategy or Approach is Defined for Data Retention &amp; Archiving</td>
<td>• Controls may not Operate Effectively</td>
<td>• Segregation of Duties Issues Exist</td>
</tr>
<tr>
<td></td>
<td>• Gaps in Controls Exist for Select Risks</td>
<td>• &quot;Roles&quot; and Assigned Responsibilities Are Not Always Aligned</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NetID Creation is Prone to Issues and Causes Workarounds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Existing Security Model Does Not Sufficiently Support the Shared Services Model</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• COA's are Inappropriately Utilized to Drive Security</td>
</tr>
</tbody>
</table>
Current State Discussion Points

Governance

Governance involves establishing standards of business conduct supported by policies and procedures with clear assignment of authority, responsibility and accountability over controls.

What we need to learn

– Who is involved with approving user access changes?
– How are roles structured? Are they well aligned with jobs/positions?
– How many roles are currently administered for EBS and DWH? How many EBS users are administered?
– Are owners assigned to roles? How are required changes to roles identified and managed? How are roles described?

Governance – discovery session

- We have defined policies but no way of enforcing them
- It would be simpler if our approval limits were the same across all systems – it is different across all of them currently
- Roles and jobs are not aligned
- Number of responsibilities/functions: “WAY too many”
- There are no role descriptions – need this going forward
- Menu of options should be limited based on your affiliation with Yale and what you are responsible for
Current State Discussion Points

Compliance & Administration

Compliance involves actions taken to address requirements associated with regulations such as HIPAA or internal Policies at Yale. Administration pertains to the ongoing efforts involved to manage and maintain systems and processes associated with security.

What we need to learn

- How are segregation of duties and controls over sensitive/private data enforced through security and monitored?
- How many people are required to administer user access to EBS?
- What are the current SLA's?
- What are the most prevalent pain points?

Compliance & Administration – discovery session

- Poorly designed from an end user perspective
- Responsibilities and naming conventions are overly complex
- Termination process is not aligned with de-provisioning requirements – there should be a workflow that alerts department LAs that folks are retiring and ask if that person’s email address/access should stay – shouldn’t have to remove each responsibility individually
- No single view to status of a request or see all access a person has
- New role and responsibility requirements are not properly controlled, often user accounts find out about new responsibilities through a provisioning request
  - needs to have a sign off / proper change of control
  - there should be a review by folks who are going to be monitoring this after its set up (i.e., functional AND technical sign off)
- There is no documentation on new responsibilities & how to evaluate a request
- There is no way of deleting responsibilities from the system – can’t clean it up
- There is no audit history to see what access people had at what time or what responsibilities they had at what time – when we are audited, we can’t provide the necessary information
Current State Discussion Points

Compliance & Administration

Compliance involves actions taken to address requirements associated with regulations such as HIPAA or internal Policies at Yale. Administration pertains to the ongoing efforts involved to manage and maintain systems and processes associated with security.

What we need to learn

- How are segregation of duties and controls over sensitive/private data enforced through security and monitored?
- How many people are required to administer user access to EBS?
- What are the current SLA’s?
- What are the most prevalent pain points?

Compliance & Administration – discovery session

- An award might have people from multiple groups, but the person administering that grant can’t access their information due to security/controls in place.
- There is so little trust that people will behave the right way, so we end up putting too much restriction on them – there should be a way to audit this information to monitor for improper access.
- “Roles” are different across systems – they could even have the same name, but that doesn’t mean they have the same level of access.
- It is a manual process to keep track of disbursement approver authority.
- New security measures needed for someone who is no longer paid at Yale, but is still involved in projects – workarounds are used to get around this currently – need a way of giving them minimal access to do their jobs.
- The workflow for the approval process does not match the hierarchy at the higher levels (typically for travel and expense).
- Internal Service Providers (dining, printing, etc.) have no approval limits – no method for approval in place – no workflow for its approval.
Current State Discussion Points

Compliance & Administration

Compliance involves actions taken to address requirements associated with regulations such as HIPAA or internal Policies at Yale. Administration pertains to the ongoing efforts involved to manage and maintain systems and processes associated with security.

What we need to learn
- How are segregation of duties and controls over sensitive/private data enforced through security and monitored?
- How many people are required to administer user access to EBS?
- What are the current SLA’s?
- What are the most prevalent pain points?

Compliance & Administration – discovery session
- There is no “hard stop” for the segregation of duties – all manual and reviewed in Oracle
- Onboarding - Difficulty with Faculty hired in February (for example), but their start date isn’t until July 1st – people need access to things before their start date, which complicates things with netIDs, expenses, etc.
- Expected turnaround time for access changes is 2 days
- All approvals are not collected before it gets to user accounts (2 day turnaround time includes getting those additional approvals)
- Aspiration: “Needs to have such great workflow that nothing is manual”
Closing and Debrief

- Review of Action Items
- Review Progress
- Participant Feedback
- Next Steps
### Action Items

<table>
<thead>
<tr>
<th>#</th>
<th>Item</th>
<th>Assigned To</th>
<th>Target Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix
Yale Authentication System (YAS) is software.

- **An Authorization infrastructure** to control access to application data consisting of three basic pieces:
  - *Custom database tables* that contain various facts necessary to discern authorizations;
  - *Custom administrative user interfaces* for populating and maintaining data in the YAS tables (YAS Wizard/YAS Builder/START/Oracle Workflow);
  - *Custom code elements that implement YAS* in the context of EBS and DWH. In DWH YAS is primarily implemented through database views. In EBS it is implemented variously as procedural code, views, and custom.pll, Oracle Forms and Oracle Reports.

- **All security is dependent on the programming of various end-user applications which are independently developed and maintained by Yale’s IT development teams.**
How does YAS work? Domains...

- **Users are associated with Data Domains**... and are assigned domains and value using the YAS Wizard or START.

- “**Domain**” are comprised of name/value pairs. The domain name itself provides the definition of the values it contains.

- There are 26 active domains. ACCESS_ORGS, CONFIDENTIAL_JOBS... etc.

- A simple example of a domain:
  
  Example Domain Name: **ACCESS_ORGS** – Data for specific Orgs that can be accessed

- Example Domain Value: **“014501” (BLDG Yale University Art Gallery)**

- A user’s ACCESS_ORGS domain *authorizes* the user to view only data that contains the domain values.

- Example: If the Org value is “014501” the green records below would be accessible:

  Row 1: 0000102.00.25815A.354001.014501
  Row 2: 0000111.00.11420A.311201.014501
  Row 3: 0000111.00.11420A.311201.014501
  Row 4: 0000111.00.11420A.351501.014502
  Row 5: 0000111.00.11420A.351501.014503
Access Provisioning – Detail View

1. Identity entered into source systems i.e. EBS HR, Banner, Development. In EBS this is an HR “Person.”
2. New NetIDs reconciled into IDM – assignment data is recorded in IDM
3. IDM provisions a new NetID
4. IDM sends the NetID and Person records to HR
5. IDM sends Identity and NetID to the ID Store
6. When Person gets NetID and Email in HR and has person type of "Employee" a process provisions an EBS User and gives it START Responsibility “Access for Myself.”
7. End user decides to send either email request for access or use START for access;
8. START/xTrain get TAC approvals/Process Owner Approvals;
9. User Accounts receives manual Email Request or START Exception;
10. Automated START request provisions User Responsibilities and YAS values
11. User Accounts Receives Manual Request or Exception
12. End user accesses EBS (or other applications) Responsibilities and data granted