

# Discovery Session

HR, Payroll, Faculty, & Student Apps– Security and Controls

October 8, 2013

# Introductions

---

## **Presentation**

---

Introductions	2
Agenda	3
Housekeeping	5
Workshop Roles	6
Objectives and Workshops	7
Control Primer	12
Current State - Control Drivers	15
Current State - Governance	17
Current State - Controls	19
Current State - Security	21
Closing and Debrief	26
Action Items	27

---


# Presentation

- ✓ **No** Technology
- ✓ Be Fully Present
- ✓ We will have one break
- ✓ Refreshments will be provided
- ✓ **No** Notes – will have designated note takers



# Workshop Roles

Role	Name / Area of Responsibility	Responsibility
Facilitators	<ul style="list-style-type: none"> <li>▪ Karen Rossetti / Security &amp; Controls Lead</li> <li>▪ Richard Rudnicki / Security &amp; Controls Lead</li> </ul>	<ul style="list-style-type: none"> <li>▪ Conduct and guide workshops</li> <li>▪ Question and challenge workshop participants when appropriate</li> <li>▪ Provide information necessary for discussion</li> </ul>
Data Collection Owners	<ul style="list-style-type: none"> <li>▪ Karen Rossetti / Security &amp; Controls Lead</li> <li>▪ Richard Rudnicki / Security &amp; Controls Lead</li> <li>▪ John DeNuzzo / Security &amp; Controls Analyst</li> </ul>	<ul style="list-style-type: none"> <li>▪ Lead the pre-work prior to the discovery workshop to collect necessary data</li> <li>▪ Be prepared to discuss source material that was collected as part of the discovery workshop discussion</li> </ul>
Participants	<b>Stakeholders</b>	<ul style="list-style-type: none"> <li>▪ Read pre-read materials</li> <li>▪ Complete pre-workshop tasks</li> <li>▪ Actively participate in sessions</li> <li>▪ Identify key points of current process and pain points</li> <li>▪ Represent your stakeholder group</li> <li>▪ Address open items promptly</li> </ul>
Team Leads	<ul style="list-style-type: none"> <li>▪ Karen Rossetti / Security &amp; Controls Lead</li> <li>▪ Richard Rudnicki / Security &amp; Controls Lead</li> </ul>	<ul style="list-style-type: none"> <li>▪ Oversee daily progress and performance of workshops</li> <li>▪ Actively participate in sessions</li> <li>▪ Communicate matters requiring attention to program management</li> </ul>
Minutes / Note Takers	<ul style="list-style-type: none"> <li>▪ XXXX</li> </ul>	<ul style="list-style-type: none"> <li>▪ Document meeting minutes, action items, and key discussion topics</li> <li>▪ Put relevant information into appropriate PMO tool</li> <li>▪ Ensure notes are published to the full audience</li> </ul>


# Objectives and Workshops




Simplify and  
standardize  
processes





Make it easy to get  
work done and harder  
to make mistakes





Workday@Yale




Establish an  
accurate, trusted and  
timely reporting  
environment



Minimize  
administrative  
overhead for faculty  
and end users

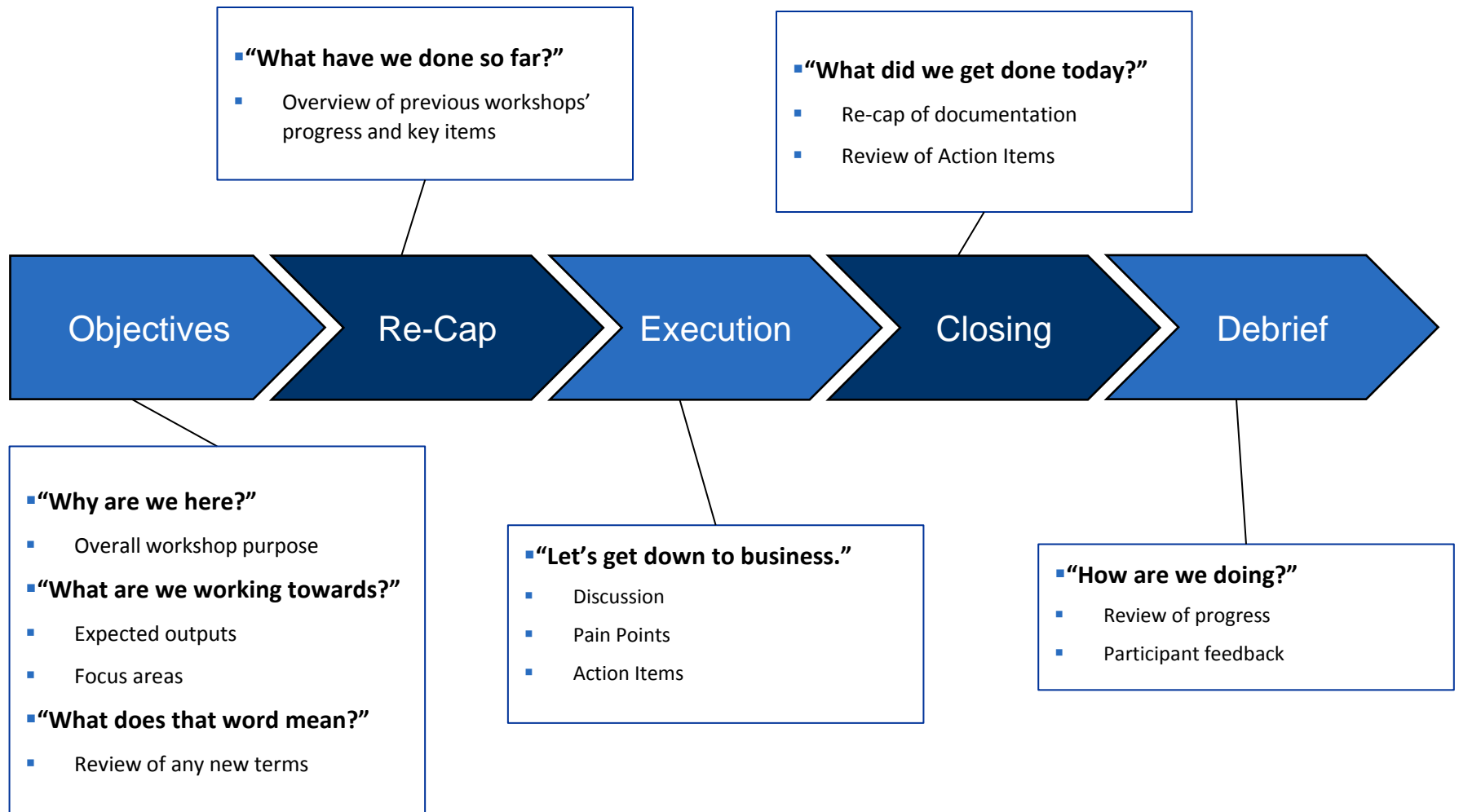


Lower operating costs  
and improve  
effectiveness



# Objectives and Workshops (cont.)

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





# Objectives and Workshops (cont.)

The Workday@Yale program will present Yale with a requirement to focus on maintaining an effective level of existing security, controls and privacy practices. It also provides an opportunity to improve them through a risk based approach that rationalizes control related efforts and utilizes automated, preventative features within the planned Workday/BI solution

## Objectives

- The objectives for the current state workshops are:
  - Document current state security and controls for Yale HR, Payroll, Faculty, & Student Applications
  - Confirm regulatory and compliance requirements
  - Shed light on people, process, and technology impacts along with current pain points associated with security and controls for Yale HR, Payroll, Faculty, & Student Applications
  - Lay foundation for future state security and controls for the Workday@Yale program.

## Workshops

- Security and Controls Discovery workshops are scheduled for the following areas:
  - Financial Applications
  - HR, Payroll and Faculty Applications
  - User Accounts Provisioning

# 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

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 pain points related to:
  - *Governance*
  - *Controls*
  - *Security (User Access)*

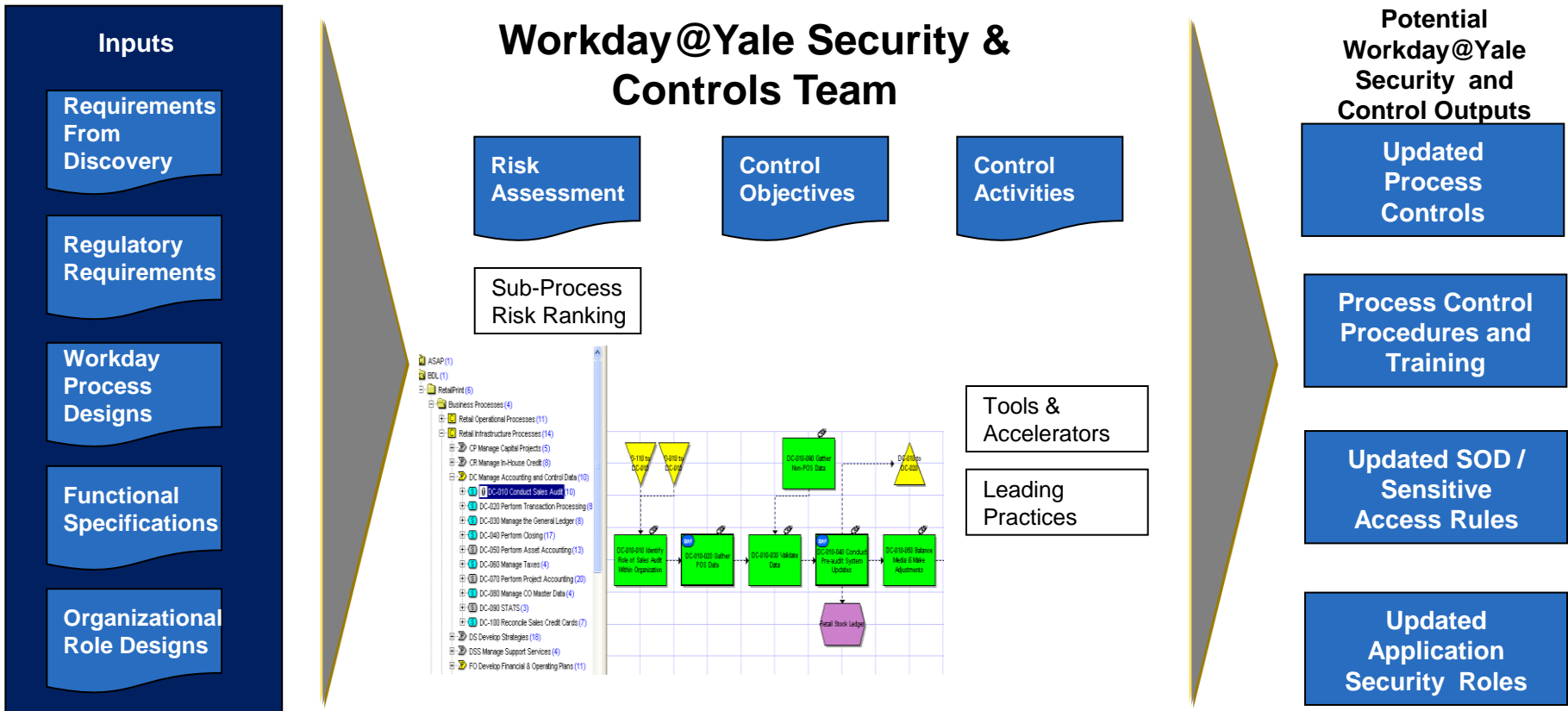
Yale must be diligent and responsible for safeguarding its assets.

## *Internal Controls*



Controls are required to protect confidential or sensitive information, maintain financial reporting integrity, manage business operations, and comply with regulatory requirements, standards and policies.

- 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.



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

Access Controls (a.k.a. Security)	<ul style="list-style-type: none"> <li>» <i>Restrict access to sensitive data and functionality</i></li> <li>» <i>Enforce segregation of duties and facilitate privacy requirements</i></li> <li>» <i>Preventative in nature</i></li> </ul>
System Enabled Controls	<ul style="list-style-type: none"> <li>» <i>Automated controls enabled through system (i.e. edits, workflows, tolerances, matching, etc.)</i></li> <li>» <i>Generally preventative in nature</i></li> </ul>
Manual/ Monitoring Controls	<ul style="list-style-type: none"> <li>» <i>Manual (documented) procedures</i></li> <li>» <i>Control / Compliance reporting and event logging / system auditing</i></li> <li>» <i>Generally detective in nature</i></li> </ul>

- 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

## Current State Control Drivers

### Compliance drivers identified to date:

- HIPAA
- FERPA
- OSHA
- Union Contract Compliance
- Reputational Risk Aversion
- Internal Sensitivity
- Yale Internal Policies
- Human & animal subjects
- Conflict of interest
- Export controls
- A-133
- A-110
- A-21
- Internal Revenue Services (IRS)
- Treasury Department
- GAAP
- FASB
- OFAC
- CHEFA
- Immigration – manual review
- Debarment and suspension
- Bayh-Dole Act
- State Tax compliance
- American recovery act
- Anti-boycotting
- Lobbying
- Agency-specific policies
- DOL
- Federal acquisition regulations
- Donor-specific policies
- FCPA
- PCI
- ISO
- COBIT
- SBA
- Federal shipping regulations

## Current State Control Drivers

### **Compliance drivers identified to date (continued):**

- Select Agents
- Office of Equal Opportunity Program(OEOP)
- Integrated Postsecondary Education Data System (IPEDS)
- I-9 compliance
- Electronic Public Health Information (ePHI)
- Affordable Care Act (ACA)
- The Office of Federal Contract Compliance Programs (OFCCP)
- Conn Dept. of Labor (State and Federal)
- Office of Environmental Health & Safety (OEHS)
- Yale Medical Group (YMG) Credentialing
- Background check
- Connecticut sick leave law
- Family Medical Leave Act (FMLA)



## 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 learned so far:

- Missing Policies that We Should Have
- Select Policies may not be Clear
- Policies are not Specific for the Roles to Which They Apply
- People move into roles without Appropriate Policy Awareness or Training
- Policies are Inconsistently Applied
- Policies not being Monitored or Followed or Enforced Properly
- Monitoring of Policies is Manual
- Review Cycle for Policies is not Consistent Across the University
- Fulfillment of Training is Difficult to Monitor
- Lack of Efficient and Effective Security Attestation Tools and Processes
- No Overarching Strategy or Approach is Defined for Data Retention & Archiving

### Governance – discovery session

- Multiple entities assuming ownership of policy, ownership is not defined,
- Competing policies exist
- Department vs. University wide policies
- Policies are complicated which results in security complications
- No definition as to “why” for policies. Policies are in place but not intuitive
- Process documentation not always available and when is, lacks explanation of why/how
- Consequences for violating controls - No definition of consequences, difficult to enforce controls
- Lessons learned from control violations are not shared with peers who have similar responsibilities. Missed learning opportunities
- Union contract compliance – Rules for bidding on jobs, annual increases, internal hiring, grievance tracking, etc are complicated and requires non-system solutions to comply

## Governance

### What we need to learn

- How are controls in the current state maintained to be relevant and appropriate?
- How are they documented?
- Have control owners been established? How are they empowered?
- How do you monitor ongoing effectiveness of security and controls?
- Are there any regulatory requirements that present compliance issues?
- Which of the current state controls are difficult and/or time consuming to perform?
- How do you prepare for audits and facilitate associated requirements?

### Governance – discovery session

- Maintenance of existing procedures is difficult to do since things continually change
- Opportunities exist to improve documentation
- For auditing purposes:
  - Audited training is a cumbersome process. Better monitoring could be used to ensure training is utilized efficiently and taken when required.
  - Redundant, multiple sources of content for training. The training process can be confusing/redundant.
- Lead administrator is not necessarily the most knowledgeable with respect to access
- User provisioning processes are difficult to complete/manage:
  - Difficult on-boarding process, very tedious to get access to doors, emails, etc.
  - Need to go to multiple places to get access (Completing the on-boarding process requires walking to multiple buildings and requires multiple roles to approve. This slows the process, it needs to be more streamlined.

## Controls

**Controls include activities and application techniques that are intended to address regulatory, financial and operating risks associated with processes. Controls are intended to help Yale achieve it's business objectives; costs of them should not outweigh the benefits they provide.**

### **What we have learned so far**

- Over Reliance on Cumbersome Manual Processes/Workflows
- Manual Control Procedures Are Often Lacking & Too Late
- Gaps in Controls Exist for Select Risks
- Controls may not Operate Effectively
- Trusting Culture – Need for Controls Viewed Negatively
- Training on Controls Is Lacking
- Lack of Transparency in Controls/Approval Process
- Controls can take Too Long & Delay Other Time Sensitive Processes
- Systems Heavily Customized to Comply with External or Regulatory Requirements. Need for Complexity not Balanced Against Risk
- Lack of Controls on Compliance Training Requirements

### **Controls – discovery session**

- No audit trail for approval of access
- Human reliance required to make sure that paid salaries are correct. Manual calculations need to be compared to system generated salaries. System has notifications feature but does not make corrections
- Reports are quality controls, employees use reports to check accuracy. It's a manual review process.

## Controls

### What we need to learn

- Describe the key automated controls you currently rely on
- Describe the key manual/monitoring controls that are in place
- Describe any issues associated with current controls. Do any introduce unnecessary complexity (i.e. lack of tolerances, complex workflows, etc.)?
- Are there any controls we should have but don't?

### Controls – discovery session

- Controls Positives:
  - Card access on the doors
  - Notifications of access expirations
- Need more controls on People in a power position within system have too much freedom. “Need control on the super user group.” Audit trails are hidden concerning configuration. People can initiate and approve.
- No controls exist on certain changes to applications (ex. KRONOS)

## Security (Access Controls)

**Security relates to a subset of controls that manages access to functionality required while enforcing proper segregation of duties and restrictions over sensitive data. Security will rely on the proper definition of roles and responsibilities in order to be assigned and maintained appropriately.**

### What we learned so far:

- Security/Data Access Model is Overly Granular and Complicated. Access Requirements can be Simplified
- Existing Security Model Does Not Sufficiently Support the Shared Services Model. Granular Access can be Problematic for YSS Contact Center Personnel
- Overly Complicated Model Can Degrade System Performance
- Provisioning is Complicated, Difficult to Administer, & Lacks Automation as People Change/Leave Roles
- Roles Are Not Standardized, Rationalized and Do Not Utilize Consistent Approaches to Manage Access Within and Across Systems
- "Roles" and Assigned Responsibilities Are Not Always Aligned
- Segregation of Duties Issues Exist

### Security – discovery session

- Employee Service Center 221 Whitney has same issue as YSS where existing security model does not allow them to operate efficiently
- Existing security model is overly granular in some areas but not granular enough in others. EX:
  - people can see SSN that don't need it for their job. Have access to things they shouldn't
- Cross function conflicts (YAS) EX:
  - access to salary for department, requires Yale access to lists of people
  - If user needs university wide access for some functions, and department access for others. EX: Access to salaries results in access to benefits too
- Classification structure doesn't support access based on your role. Job titles are too generic; too many positions
- Different security models exist for different groups of systems. Models are administered differently and by different people. EX: BMS HR, Oracle EBS, ALICE
- Provost office has a need to maintain confidentiality of certain information

## Security (Access Controls)

### What we need to learn

- Describe key data security requirements?
  - How is the business involved in maintain roles?
  - What are common issues associated with access?
- Chairs of departments don't have role in HR system. Annual Faculty salary increase process is manual
  - Provisioning of central responsibilities is manual process, relies on emails, without visibility to status of request.
  - Issues with roles being delegated to others because person who should be fulfilling it decided they want the business manager doing it, permanent delegation. There are issues with the process for assigning temporary and permanent delegates. When roles are delegated, there's no formal documentation of that delegation, "there's no place for it to be done."
    - Temporary coverage sometimes needed when TAC or other approval authority is on vacation, etc. requirement for workflow. Need workflow around this.
    - Controls in need to be in place to prove detect a security breach. What do we have to do for reasonable protection?
  - Audit requirement- formal documentation of delegation. No form on central side of campus.

## Security (Access Controls)

### What we need to learn (cont'd)

- Describe key data security requirements?
- How is the business involved in maintain roles?
- What are common issues associated with access?

### Security – discovery session

- Onboarding - Access to certain systems needed 90 days in advance of hire date
- PIN creation process for a NetID is semi-manual and activation not always timely
- Developers need to be able to troubleshoot problems and fix data problems within system
- If not done through access controls, need some way to filter data for end users
- Off-boarding –Yale needs automated processes for de-provisioning access based upon changes in a persons status at the university:
  - Need different processes for employees who retire/terminated/on leave
  - Employees in layoff status need netid in order to retain bidding rights on positions
  - Need automation and business processes for employees who move within the University (transfer)
  - Need future end-dating. Inability to tell the system someone will be leaving in the future.
- Training is a prerequisite to gain access to some functions
- Training fulfillment doesn't follow a user when he/she changes positions

## Security (Access Controls)

### What we need to learn (cont'd)

- Describe key data security requirements?
- How is the business involved in maintain roles?
- What are common issues associated with access?

### Security – discovery session

- Directory settings in HR should drive which information is private - SSN, salary, benefits, date of birth, home address. Needs more restriction
- FERPA – Privacy flag propagated from banner system to HR. Lack of understanding on the relationship between Banner and HR, and how to administer private student data within HR and downstream applications
- If confidential payroll is included in Workday, security will be needed to enforce confidentiality
- Replication of data in multiple systems is problematic and can result in multiple versions of truth. Rules around authoritative sources of identity data throughout a person's affiliation with the University are needed (e.g. students shouldn't be able to change their address in HR. These changes should be made through the Registrar)
- No audit trail for approval of access
- Need central view of access beyond Oracle and DWH (e.g to include MyTime, Benefits system, Recruitment system, etc...)



## Security (Access Controls)

### What we need to learn (cont'd)

- Describe key data security requirements?
- How is the business involved in maintain roles?
- What are common issues associated with access?

### Security – discovery session

- In BMS merit system, can create separate security groupings outside of the hierarchy
- Departments need to testify that Account Holders are getting financial statements. There should be an Account Holder role and system should automatically distribute statements instead of it being a manual process.
- Today we have the ability to secure data by multiple dimensions – job, organization, project, etc...Will we need this level of complexity going forward?

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

#	Item	Assigned To	Target Due Date
1	Meet with Rich Jacobs – Federal liaison		
2			
3			
4			
5			
6			
7			
8			
9			