

Discovery Session

Financial Applications – Security and Controls

October 2, 2013

Introductions

Presentation

Introductions	2
Agenda	3
Housekeeping	5
Workshop Roles	6
Objectives and Workshops	7
Security & Controls Vision Plan Objectives	11
Activities to Date	12
Control Primer	13
What's Been Learned	16
Current State – Control Drivers	17
Current State - Governance	18
Current State - Controls	20
Current State - Security	22
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"> ▪ Karen Rossetti / Security & Controls Lead ▪ Richard Rudnicki / Security & Controls Lead 	<ul style="list-style-type: none"> ▪ Conduct and guide workshops ▪ Question and challenge workshop participants when appropriate ▪ Provide information necessary for discussion
Data Collection Owners	<ul style="list-style-type: none"> ▪ Karen Rossetti / Security & Controls Lead ▪ Richard Rudnicki / Security & Controls Lead ▪ John DeNuzzo / Security & Controls Analyst 	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Karen Rossetti / Security & Controls Lead ▪ Richard Rudnicki / Security & Controls Lead 	<ul style="list-style-type: none"> ▪ Oversee daily progress and performance of workshops ▪ Actively participate in sessions ▪ Communicate matters requiring attention to program management
Minutes / Note Takers	<ul style="list-style-type: none"> ▪ Ross Dodd 	<ul style="list-style-type: none"> ▪ 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





Workday@Yale




Establish an
accurate, trusted and
timely reporting
environment



Minimize
administrative
overhead for faculty
and end users

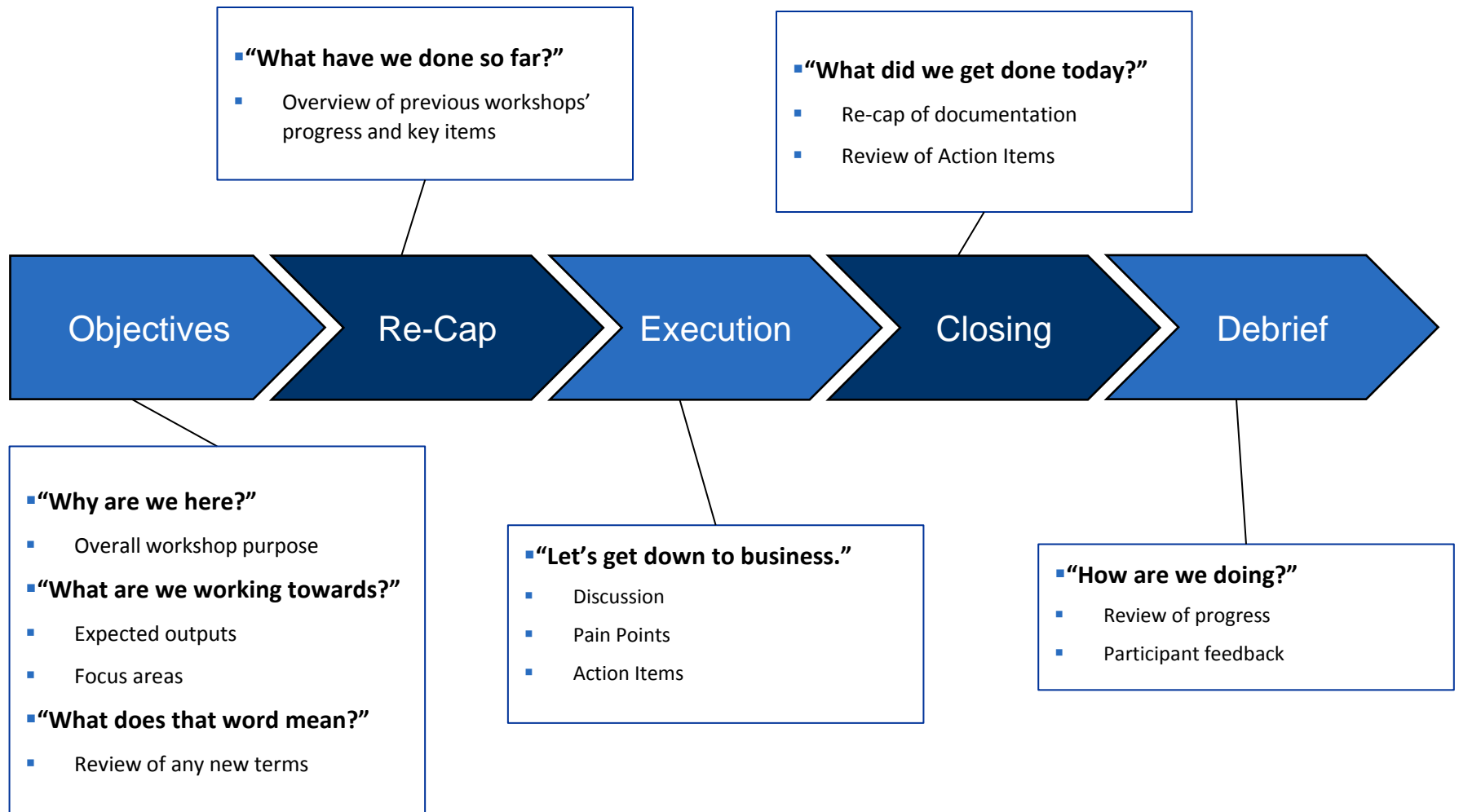


Lower operating costs
and improve
effectiveness



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 Finance 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 Finance 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

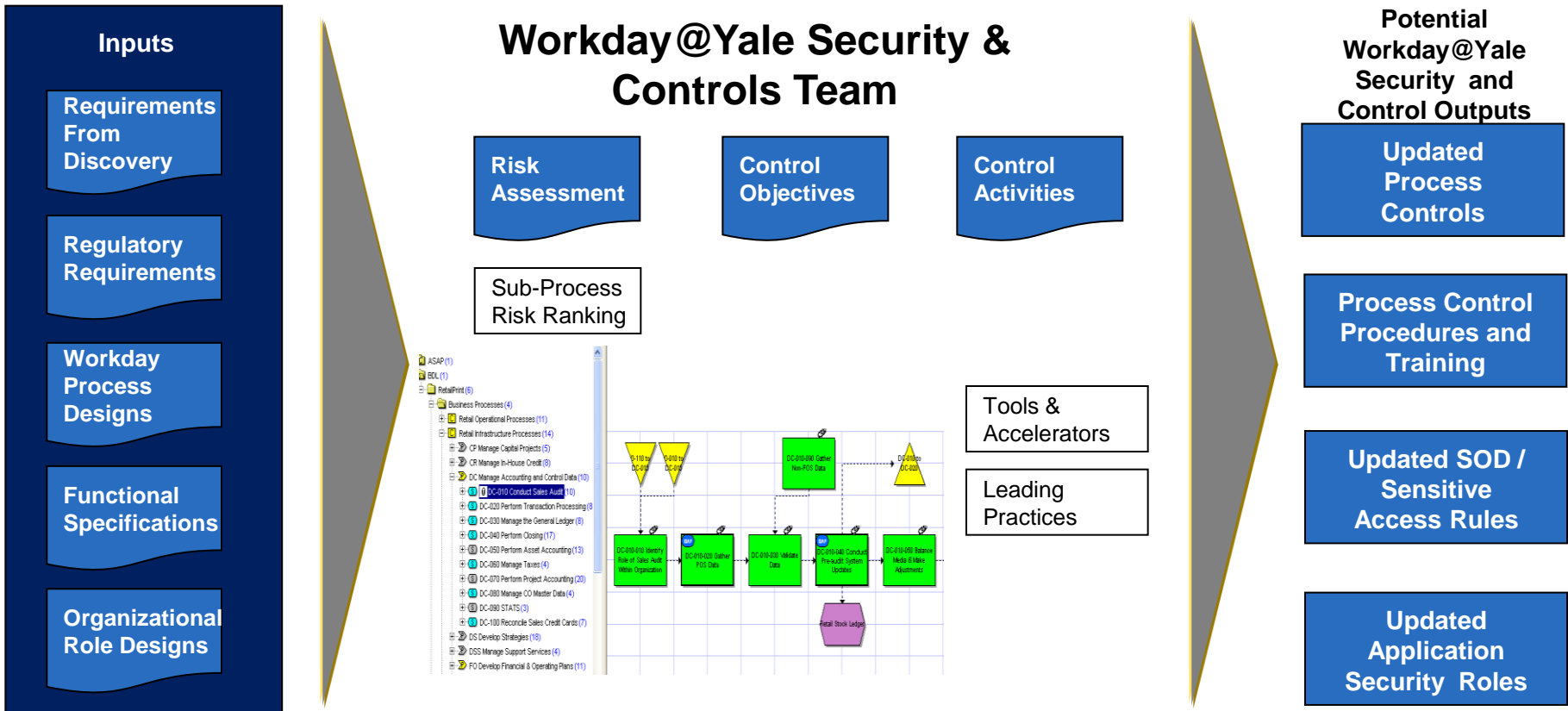
RESOLVE relevant open action items prior to and during meetings to further progress of the workshops as a whole

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

- 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*

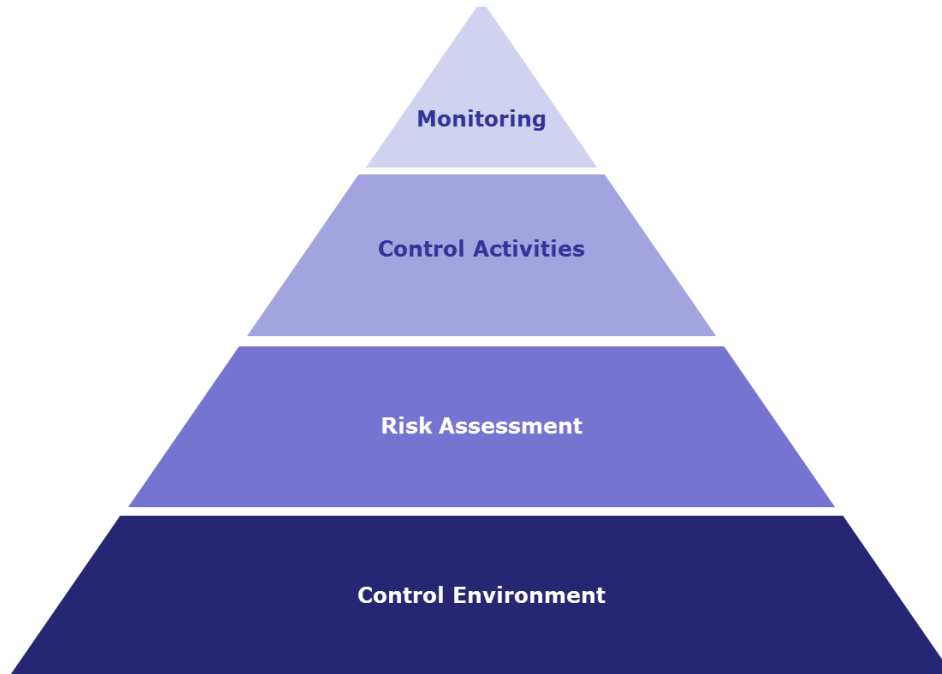
Topics to be Considered

Topics that should be considered in today's session:

- Level set on controls
- Review pain point emerging themes
- Identify other pain points related to:
 - *Governance*
 - *Controls*
 - *Security (User Access)*

Yale must be diligent and responsible for safeguarding its assets.

Internal Controls



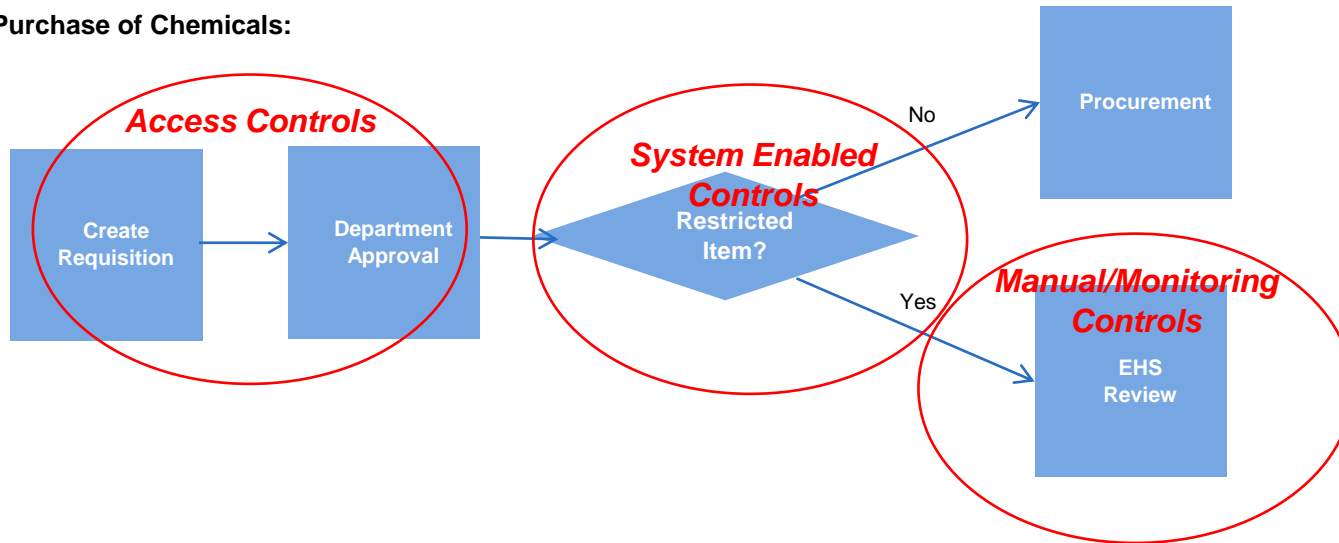
Consistent with the Planning & Financial Management Program (PFM), the Workday@Yale program will need to consider internal controls to safeguard assets and help meet business objectives.

- 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:

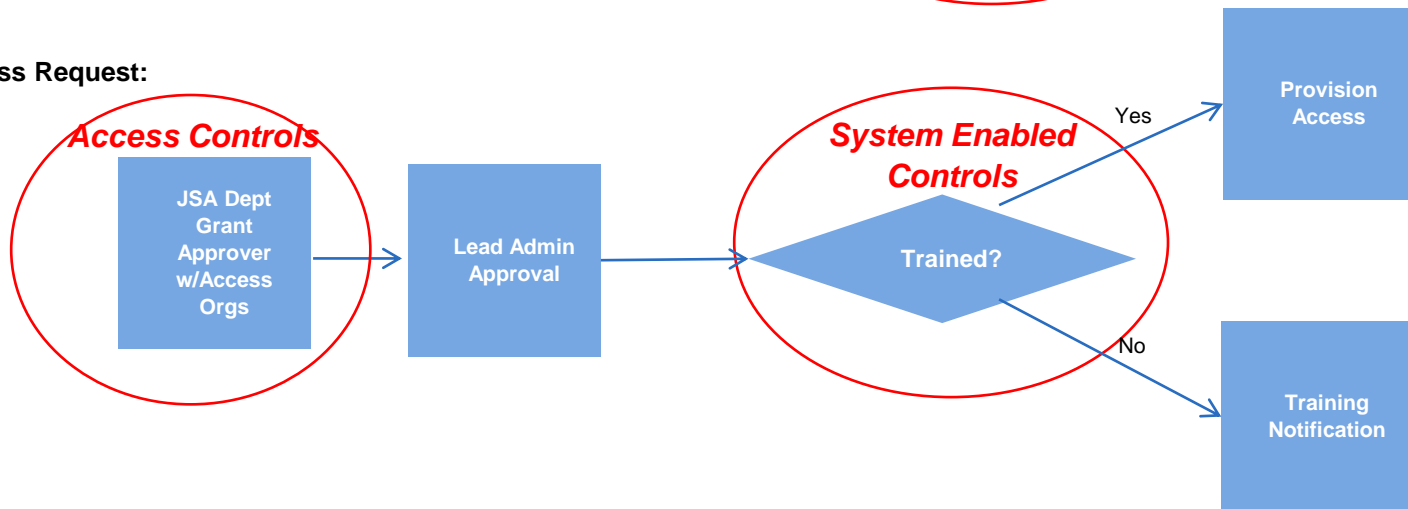
Access Controls (a.k.a. Security)	<ul style="list-style-type: none">» <i>Restrict access to sensitive data and functionality</i>» <i>Enforce segregation of duties and facilitate privacy requirements</i>» <i>Preventative in nature</i>
System Enabled Controls	<ul style="list-style-type: none">» <i>Automated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

- 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

#1 – Purchase of Chemicals:



#2 – System Access Request:



Pain Points – Emerging Themes:

Governance	Controls	Security (Access Controls)
<ul style="list-style-type: none">• Select Policies May Not be Clear or Enforced Properly• 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 (project underway for libraries and others archiving documentation)	<ul style="list-style-type: none">• Over Reliance on Cumbersome Manual Processes/Workflows• Manual Control Procedures Are Often Lacking• Specific Training on Controls Is Lacking• Controls may not Operate Effectively• Gaps in Controls Exist for Select Risks	<ul style="list-style-type: none">• Security/Data Access Model is Overly Granular and Complicated to Administer• Provisioning is Complicated and Difficult to Administer• Roles Are Not Standardized, Rationalized and Do Not Utilize Consistent Approaches to Manage Access Within and Across Systems• Segregation of Duties Issues Exist• "Roles" and Assigned Responsibilities Are Not Always Aligned• NetID Creation is Prone to Issues and Causes Workarounds• Existing Security Model Does Not Sufficiently Support the Shared Services Model• COA's are Inappropriately Utilized to Drive Security

Current State Control Drivers

Compliance drivers identified to date.

- A-133
- A-110 (implemented differently by agencies)
- A-21
- Human & animal subjects
- OSHA
- Conflict of interest
- Export controls
- HIPAA
- FERPA
- Internal Revenue Services (IRS)
- Treasury Department
- GAAP
- FASB
- OFAC
- CHEFA
- Reputational Risk Aversion
- Internal Sensitivity
- Yale Internal Policies

Compliance drivers – discovery session

- 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
- Select agents

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

- 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

- Missing policies that we should have in addition to those that are unclear
- Policies not being monitored or followed
- Review cycle for policies is not consistent across the university
- Would be nice if there were guidelines or (required) training around our policies – people coming into roles without appropriate policy awareness
- Policies are not specific enough to the roles to which they apply
- Policies are inconsistently applied with no enforcement/override at higher level (balancing “policy as written” with reality)
- Approval limits are inconsistent across systems- e.g. SciQuest, EMS
- SOD- Lead Administrators are responsible for compliance, but are not empowered to define/change the process

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

- 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

- There are too many “roles’ (responsibilities/functions) and it is unclear what is entailed in each
- There should be overarching guidance around, depending on a role, who has access to what data
- Had to heavily customize our systems to comply with external or regulatory requirements
- When there is an audit, there is generally a point person for that audit with support from other areas at Yale (e.g., general counsel, etc.)
 - Healthcare audits go through Yale medical
- Its hard to see the segregation of duties with Oracle currently
- We have a culture that is very trusting and could regard internal controls as insulting – misunderstanding of why policy is implemented
- When people are requesting to make changes to responsibilities, the changes need to be vetted through the process owner – room for improvement here

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 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

- Rely on/use Access Review Report
- We don't have great tools to handle controls; there are multiple places to send requests - minimal automation that rarely work anyway
- Lack of workflow requires manual workaround
- Perception that costs of compliance outweigh the benefit
- System controls force a standardization of controls that are not always needed. System controls enforce complex security requirements based on regulations. Often this is applied in areas where that level of complexity it not necessary, hampering the process
- Award end dates are prohibitive– Payments are received well after them and have to go back in to change them
- Most of the controls are after the fact and in some cases, it is too late for those controls to be enforced
- Sometime the control point takes too long and is unpredictable, which can delay other time sensitive processes e.g. contract approvals for sub-recipients
- Lack of transparency in the controls approval process (e.g., if my request is delayed, why is it delayed?)
- Manual process for monitoring policy compliance makes it difficult/slower to enforce

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 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

- Disconnect between START and XTrain – any approvals in START do not convey over to Xtrain
- When inputs come in multiple forms (e.g., electronic invoices vs. paper invoices that are duplicates), makes the controls process for proper payment more difficult
- Reviewing the hold report is a good way of zeroing in on some of the controls
- Documentation on customizations that have been done in the system is lacking
- In order to save effort, we might create control workarounds that we don't realize affects things later on in the process
- System controls focus on what can/cannot be charged to a sponsored award. Non financial system controls are lacking (COI, F&A, patent policies, training etc.)
- Lack of controls on compliance training requirements for lab personnel
- Manual controls that are in place for tax require a lot of technical knowledge and the rules are dynamic
- Monitoring that goes on with sub-recipients
- Procurement is all manual for review (thousands of people who have access) – we don't know what level of view these people have

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 need to learn

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

Security – discovery session

- Access is granted inconsistently across roles; often assigned based upon what someone else has
- Complexity - There are cases depending, on what the access requirements are, where it should be complicated, but in most cases, it should be simpler
- Need for granularity around salaries and confidential data tied to vendors (e.g., bank account numbers), but not necessary for other data
- Security needed to protect Yale's image (e.g. animal research purchases)
- Security helps to filter data for users, making it easier for them to get to the data they need
- Complexity of access model creates conflicts for people whose job requires them to have both university level and department level access
- Specifics to charging and owning org would benefit from a combined view
- System availability and its response once accessed
- We want a simple process where we can see what access a person has along with an audit trail
- We need role-based security
- There should be notifications around separations to make sure we know when to restrict access
- SOD – Preparers can be approvers in many applications

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 need to learn

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

Security – discovery session

- Room for improvement in role provisioning for 3rd party applications and how they “talk” to our other applications with regards to roles and their access
- Responsibilities/functions are not intuitively named
- If there are any changes made in the system, the system should know if there are any access conflicts
- Sometimes we need multiple roles to perform our jobs
- Approval limits in systems are not aligned – some require more than others
- We should be able to delegate temporary access when a key person is not available (some applications have this, most don't) – need controls around who can delegate to who and an audit trail to see what access people had at what times – need to be able to set end dates for delegations
- For PIs that delegate authority, there is no effective ways for departments to administer this
- Need definition and controls around temporary delegation vs. permanent
- With agency employees, there is a broken piece in the automation of netIDs that causes the process to become manual

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 need to learn

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

Security – discovery session

- You can set up Net IDs before an employee starts, but the employee themselves have to activate – they don't always activate it
- Employees set up in HR without an email address renders EMS workflow ineffective
- YSS contact center needs to have all sorts of access in order to answer their requests, but if there isn't a view-only, then we have to customize the responsibility. We need instances where responsibilities overlap for these individuals or else multiple people are needed to address the request – cant do this currently unless you are higher up in YSS
- There is an interrelation between downstream applications that forces us to have certain levels of security
- We are considering role-based security, but some departments aren't organized roles. They manage by portfolios e.g. manage a group of faculty
- Over-complication of security model can slow the performance of the system
- Need auditing trail on changes to fields or transactions – we can only see who updated, not what they updated

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 need to learn

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

Security – discovery session

- MFT, Unix and Windows provisioning is administered differently depending on the organization – it is not clear what group gives access to what directories
- Reference domain access is a challenge – need a one stop shop for setting up access
- Need to consider whether the process supports compounding access
- We have no way of tagging information to know how long we should retain it (archiving strategy)
- On-boarding/Off-boarding and proper access control is difficult
 - Not easy to monitor access because data pertaining to end dates is not always complete or correct
 - There needs to be something in HR that triggers an action for changing/eliminating someone's access
- Conflict between business functions with university wide views

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

#	Item	Assigned To	Target Due Date
1			
2			
3			
4			
5			
6			
7			
8			
9			