MIS 5121: Enterprise Resource Planning Systems
Week 11: *Change Management, IT Controls Framework*
MIS 5121: Upcoming Events

- Exercise 4 (Segregation of Duties) – *Past Due*: April 2
- Reading Assignment 7 – *Past Due*: April 5
- **Exam 2** – In class: *April 6 (today)*

- Reading Assignment 8 – *Due*: April 12

- Reading Assignment 9 – *Due*: April 19 (Week Earlier)
Control Failure: Deepan Patel’s Presentation

- **Background:**
  - 
  - 

- **Control Failures: 2006 – 2009**
  - 
  - 

- **Results:**
  - 
  - 

- **Reference:**
  - 
  -
Control Failure: Ivy Zhu’s Presentation

• **Background:**
  -
  -

• **Control Failures: 2006 – 2009**
  -
  -

• **Results:**
  -
  -

• **Reference:**
  -
Control Failure: Jingyi Zhou’s Presentation

• **Background:**
  - 
  -

• **Control Failures: 2006 – 2009**
  - 
  -

• **Results:**
  - 
  -

• **Reference:**
  -
Change Management
SAP: Transport Management
Typical SAP Landscape

- Development System
  - Type of Users:
    -
    -
    -
  - Type of Work:
    -
    -
    -

- Quality-Assurance System
  - Type of Users:
    -
    -
    -
  - Type of Work:
    -
    -
    -

- Production System
  - Type of Users:
    -
    -
    -
  - Type of Work:
    -
    -
    -
Typical SAP Landscape

**Development System**
- Type of users: Developers, Consultants, Key Users
- Type of work: Customizing, Development, Unit Testing

**Quality-Assurance System**
- Type of users: Developers, Consultants, Key Users
- Type of work: Integration and Quality testing

**Production System**
- Type of users: End users
- Type of work: Productive execution of transactions with real business data

Developments, corrections & customizing settings
SAP Landscape: Instance and Clients

• **SAP Instance**
  – Instance also referred to as a system
  – An Instance has a dedicated physical database
  – One installation of SAP software (source code / modules) and related logical database is an instance
  – Instance shares SAP and developed software ‘code’ base
  – Documentation of instances (systems) and clients often called: ‘**Client / System Landscape**’
Minimum Rec’d SAP Landscape
SAP Landscape: Instance and Clients

• **SAP Clients**
  – Client is highest organization level with SAP System
  – At least one client per system (e.g. ‘100’)
  – Master data is stored and Business transactions occur within a client
  – Single logical database (linked to system / instance) may contain several clients
  – Production Client typically represents a logical grouping of multiple companies
Client Dependent vs. Independent

**System/Instance**

**Client Dependent**

- Dev 100 Master (Gold)
  - Master Data
  - Transaction Data
  - User Management / Data
- Dev 110 Dev Test
  - Master Data
  - Transaction Data
  - User Management / Data
- Dev 180 Data Conversion
  - Master Data
  - Transaction Data
  - User Management / Data
- Dev 900 Sandbox
  - Master Data
  - Transaction Data
  - User Management / Data

**Client Independent**

- Programs (ABAP) > Repository Objects (Client Independent Config)
  - Currency, UOM’s
  - Pricing Tables
- Data Dictionary
- Parameters
- Authorization Objects > Transactions
SAP Change Management

- SAP’s Correction and Transport System (CTS) provides framework for proper change control process
- SAP’s TMS (Transport Management System) is subset of CTS
- TMS Transport Routes / Paths (transaction STMS) move changes between Clients / Instances (e.g. to test, Production)
- Transaction STMS
SAP Change Management

- System changes on save Prompt for Transport Request (New or include in prior ‘open’ request)
- Transport in addition to change meta data (creator, create date/time) includes details of the change
  - Configuration table entries (changes)
  - Development object (code change)
- Assigns unique transport Number
TMS Terminology

- Transport (the truck icon): contains the changes (including role changes) moved from client to client and system to system per transport path.
- User ‘owns’ the change request and it’s details.
- User must ‘release’ transport prior to migration.
Note: For any given change, the **same** change is moved / migrated to **each** system. Changes are not moved from system to system.
Transport Paths

- TMS Transport Routes / Paths define logical connections between the different systems in an environment.
- System changes moved to systems along these pre-defined transport paths.
- Paths typically defined during initial landscape design and implementation.
Transport Process

- Actual import occurs at the operating system level (SAP Basis)
- Administrator defines start time
- Defined start time (midnight? 4 pm, ??)
- Defined Procedure for administrator to choose requests (based on testing status, approvals, etc.)
- All transport errors must be reviewed and corrected if necessary
Transport Security

- Access to TMS highly restricted to system administrators
- Development classes can be associated with transports
- Segregation of duties
  - Ability to change vs. release transports
  - Ability to change / release vs. migration
Transport Controls

- Transporting changes into production access is restricted to authorized personnel via SAP Security
- All changes entering production environment adequately supported by:
  - Change approvals by appropriate personnel
  - Documentation of change (e.g. SAP Solution Manager)
  - Test results
- Review transport paths and related procedures to ensure appropriate change controls are designed and used to modify them
SAP Landscape: Instance Security

- Also referred to as ‘Application Server Parameters’
- Need to be configured on each logical instance
- Must review parameters on all application servers
- Default SAP Parameters do not provide adequate level of security
- May vary depending on business’s Security Policies
# Critical Instance Profile Parameters

<table>
<thead>
<tr>
<th>Parameter / Description</th>
<th>SAP Default</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login/min_password_lng</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Minimum password length</td>
<td></td>
<td></td>
</tr>
<tr>
<td># days after which password must change</td>
<td>0</td>
<td>30-60 Days</td>
</tr>
<tr>
<td>Login/fails_to_session_end</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Login/fails_to_user_lock</td>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>Login/failed_user_auto_unlock</td>
<td>1 (Auto unlock)</td>
<td>0 (remains locked)</td>
</tr>
</tbody>
</table>
## Critical Instance Profile Parameters

<table>
<thead>
<tr>
<th>Parameter / Description</th>
<th>SAP Default</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth/rgc_authority_check</td>
<td>0</td>
<td>1 (RFC’s are checked)</td>
</tr>
<tr>
<td>Check authorization for remote function calls (Client/system to other)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rdisp/gui_auto_logout</td>
<td>0</td>
<td>3600</td>
</tr>
<tr>
<td># seconds to auto disconnect inactive users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login/disable_multi_gui_Login</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Block multi logon if set to 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Setting System Change Options

• Transaction: SE06
• Changes affect entire system / instance
• Affects Client Independent objects
• PRD Global setting should be ‘Not Modifiable’
Client Dependent vs. Independent

**System/Instance**

### Client Dependent

- **Dev 100** Master (Gold)
  - Master Data
  - Transaction Data
  - User Management / Data

- **Dev 110** Dev Test
  - Master Data
  - Transaction Data
  - User Management / Data

- **Dev 180** Data Conversion
  - Master Data
  - Transaction Data
  - User Management / Data

- **Dev 900** Sandbox
  - Master Data
  - Transaction Data
  - User Management / Data

### Client Independent

- Programs (ABAP)  > Repository Objects (Client Independent Config)
  - Currency, UOM’s
  - Pricing Tables

- Data Dictionary

- Parameters

- Authorization Objects  > Transactions
Setting System Change Options

- Client Independent Object Modifiable if these parameters are ‘Modifiable’

  - Global Setting
  - Software component of object

  - Namespace or Name Range
## Setting System Change Options

- **Transaction:** SE06

### Software Component

<table>
<thead>
<tr>
<th></th>
<th>Modifiable</th>
<th>Restricted</th>
<th>Not Modifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Namespace</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modifiable</td>
<td>Existing Objects can be changed</td>
<td>Existing objects can be repaired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New objects have SAP System ID of original System</td>
<td>New objects have SAP System ID of original System</td>
<td></td>
</tr>
<tr>
<td>Not Modifiable</td>
<td></td>
<td></td>
<td><strong>No Changes Possible</strong></td>
</tr>
</tbody>
</table>
Risk and Recommendation

Instance Profile Parameters

Risks:

SAP Default settings do not provide adequate control over system.
Settings not configured could result in system’s security being compromised and unauthorized access

Recommendations:

Review all parameter values different than recommended – understand why company has chosen non-recommended value
PRD (Production) Instance Security

- Focus of audits are the PRD System
- PRD often the standalone environment referred to as the ‘Live’ system
- Only thoroughly tested configuration changes should be transported to PRD to assure integrity of this environment
- No configuration access should be allowed in PRD
- Direct changes in PRD (Occasionally required) handled with strict policies, procedures, approvals.
Setting System Security: Clients

- Transaction: SCC4
- Settings for all clients in an instance
- May be different btw DEV & PRD
- PRD should be ‘No Change Allowed’
- Options authorized per security Policy / Procedures
- Only system administrator able to change options
- Process for system open/close
  - Defined / Documented
  - Rarely used
  - Closely Monitored
Setting System (Client) Security

**Recd:** ‘No Changes Allowed’ in PRD to prevent unauthorized changes to Client-specific objects

**Recd:** ‘No Changes to Repository and Cross-client customizing Objs’ in PRD to prevent unauthorized changes to Client-independent objects

**Recd:** Level 1 or 2 in PRD to prevent overwriting when using client copy or client comparison tools
Change Management / Transport Management Overview

- Client dependent vs. Client independent objects / components

- Transport Process
  - Transports
  - Transport Paths
  - Activities
  - Controls

- Instance / Client Security: Risks & Recommendations
Assignment Questions

- How do clients in the SAP system fit in the change management process?
- When we audit, how we could know if it is the right “change management” to detect the fraud?
- What is the relation between change management and the development life cycle of software?
- Why is it difficult to make changes to a live SAP system or any business application?
- Do you think change management could be successful without full documentation? Why or why not?
- What is the reason for dearth of know-how in SAP Solution Manager (SM) implementation? Why would organizations not take advantage of the free offer and direct funds for training and talent? If absence of SAP Solution Mgr means negative audit finding, does that mean it is mandatory?
- Considering SAP’s design and what we know about it and what we know about the role of IT departments, does SAP provide sufficient general IT controls either explicitly or by design? How so?
ERP Systems and Shared Services
Shared Service Models

- What are they?

- Why Use / Implement?

- Goals?
Shared Service Models
(One Taxonomy)

- **Outsourcing**: Sending job functions outside organization (vs. in-house)
  - Off-shore: Services performed offshore
  - Near-shore / On-shore: Services performed outside but relatively nearby
- **Insourcing**: delegating work to internal resources (vs. outsourcing)
- **Co-sourcing**: Collaborative partnering (shared risk?)
- **Mixed models**
Shared Service Controls ?’s

- How can I better define my audits in the new environment?
- Do the controls now reside at the SSC or in the business units?
- Are the processes and templates used across the SSC consistent? Do work-arounds proliferate?
- Can I use automation in the audit process more effectively now that I am auditing in an SSC environment?
- What is the steady state assurance strategy? (Who will provide monitoring and assurance, and what is the scope?)
- What audit clauses exist contractually for a SSC?
- Are you able to measure risk exposure for each service provider?
- Does a steady state governance structure exist to manage the shared services and the outsourcing arrangements?

**SSC: Shared Service Center**
Shared Service Management Principles (ENB)

- The operations of the process in SSC can be delegated to a service organization
  - Contractual commitments
  - Defined Goals and SLA’s (Service Level Agreements)
  - Cooperative management

- Control mechanisms in SSC run processes ultimately remain the **responsibility** of the business / client
  - SSC can administer and monitor process controls
  - Design and ultimate sign-off by the business / client

- Process Design of critical processes must be ‘owned’ by the business / client
Shared Service Management Principles (ENB)

- Certification by SS provider is useful
  - Independent assessment / evaluation
  - Defined measures & standards
  - Business / Client needs to understand what certification means / doesn’t

- Process / Expectation Documentation is critical
- Define the strategic reasons for the SS Change – Align to business goals
- Benchmark wherever possible
- On-going Assessment / Process Improvement Mindset
ERP Systems and Shared Services

Top Reasons for Outsourcing

- Reduce Costs: 36%
- Focus on Core: 36%
- Improve Quality: 13%
- Increase Speed to Market: 10%
- Foster Innovation: 4%
- Conserve Capital: 1%

Source: The 2001 Outsourcing World Summit
ERP Systems and Shared Services

• 2+ Principles
Assignment Questions

- How to monitor the outsourced controls? Is there a specific function controlling that in SAP?
- Can SAP configuration include certification requirements?
- Can an organization rely on the outsourcer SLAs and contract terms to support its own internal control environment? What precautions should be taken into account?
- How often should an SLA agreement be reviewed?
- Would you outsource and displace a lot of employees to save a dollar?
- I have a general idea from the reading of ISAI 3402 and SAS 70. As an auditor, would need to know in great detail? Specifically the control mechanisms within each and how they can be applied to SAP ERP.
- When we outsource the IT functions, what frameworks and controls are used to manage vendor risks? Which one is the most effective?
Break Time
Risk / Control Matrix
Final Exercise
COSO Framework (2013)
## COSO Framework (2013)

### Codification of 17 principles embedded in the original Framework

<table>
<thead>
<tr>
<th>Section</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Environment</strong></td>
<td>1. Demonstrates commitment to integrity and ethical values</td>
</tr>
<tr>
<td></td>
<td>2. Exercises oversight responsibility</td>
</tr>
<tr>
<td></td>
<td>3. Establishes structure, authority and responsibility</td>
</tr>
<tr>
<td></td>
<td>4. Demonstrates commitment to competence</td>
</tr>
<tr>
<td></td>
<td>5. Enforces accountability</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>6. Specifies relevant objectives</td>
</tr>
<tr>
<td></td>
<td>7. Identifies and analyzes risk</td>
</tr>
<tr>
<td></td>
<td>8. Assesses fraud risk</td>
</tr>
<tr>
<td></td>
<td>9. Identifies and analyzes significant change</td>
</tr>
<tr>
<td><strong>Control Activities</strong></td>
<td>10. Selects and develops control activities</td>
</tr>
<tr>
<td></td>
<td>11. Selects and develops general controls over technology</td>
</tr>
<tr>
<td></td>
<td>12. Deploys through policies and procedures</td>
</tr>
<tr>
<td><strong>Information &amp; Communication</strong></td>
<td>13. Uses relevant information</td>
</tr>
<tr>
<td></td>
<td>14. Communicates internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicates externally</td>
</tr>
<tr>
<td><strong>Monitoring Activities</strong></td>
<td>16. Conducts ongoing and/or separate evaluations</td>
</tr>
<tr>
<td></td>
<td>17. Evaluates and communicates deficiencies</td>
</tr>
</tbody>
</table>
Risk / Control Matrix: Final Exercise

Parts

1. Analyze and define the key risks that exist for the Order to Cash (OTC) process at GBI.
2. Guided by the risks you identified (esp. the High Severity and High Likelihood / Frequency risks) identify the key controls that will be used in the OTC process.
3. Link the Risks from Part 1 to the controls in Part 2.
4. Complete definition of the controls (classifications, links to assertions, etc.)
5. Write auditable control process documentation for 1 manual and 1 automated (configuration) control identified.
6. (Individual vs. Team submission): Couple questions about your work as a team to complete this a other exercises.
Risk / Control Matrix: Final Exercise

• Agenda
  – This Class (April 6): Part 1 (Identify Risks)
  – Future Class (April 13): Part 2, 3 (Identify Controls, Link Controls to Risks)
  – Future Class (April 20): Part 4 (Complete Control Definitions)
  – Future Class (April 27): Part 5, 6 (Control Process / Audit Details; Personal Questions)
  – Due April 30 11:59 PM: Assignment Submission
Risk / Control Matrix: Final Exercise

Part 1:

a) Analyze the key risks that exist for the Order to Cash (OTC) process at GBI

b) Define and document the key risks that exist for the Order to Cash (OTC) process at GBI

- Tab: Part 1 – GBI Risks
- Identify at minimum 25 risks in the process
- Identify a minimum 4 risks in each of the OTC sub-processes:
  - **OR&H**: Order Receipt and Handling
  - **MF**: Material Flow (shipping)
  - **CI**: Customer Invoicing
  - **PR&H**: Payment Receipt and Handling
Extra Slides
Extra Slides

Threat Level

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Risk Assessment

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Significant</td>
<td>Extensive Management Essential</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td>Management Effort Required</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Acceptable Risks</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td>Accept and Monitor Risks</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Manage &amp; Monitor Risks</td>
</tr>
</tbody>
</table>
Change Documents

- Change ‘log’ stores information on changes made to master data and transaction data via standard transactions (Miss direct table maintenance changes)
- Permanent record and audit trail for transactions executed in SAP
Risk and Recommendation
Change Documents

Risks:
If users are not restricted from maintaining change documents, the system audit trail from changes documents could be deleted accidentally or via malicious intent.

Recommendations:
Users in production have activity level of security object S_SCD0 set to ‘08’ (Display Change Documents). Investigate ways access to maintenance of change documents could be further restricted (locking transaction)