MIS 5121: Business Processes, ERP Systems & Controls
Week 12: System Development Controls
Exam 2 Test Results

- Results will be ‘curved’ to Max high score vs. perfect score of 38.25
- Final Exam will have long time limit
Procurement at GBI
Purchase to Pay Process
The Many Flavors of Procurement

• Materials / Raw Materials
• Labor Services
• Other Services
• Leases / Rentals
• Supplies (Office, Maintenance, Production, …)
• Logistics
• Information Technology
• No PO
• Inter-company vs. 3rd Party
• Acquisitions
Order to Cash at GBI

Marketing / Sales

Customer Service

Order

Inquiry

Supply Chain

Conversion

Procurement

Warehouse Distribution

Delivery / Shipment

Invoice

Finance / HR

Billing

Accounts Receivable

Payment

Accounts Payable

Customers

Suppliers
The Many Flavors of Sales Order

• Standard Orders
• Free of Charge (samples, compensation)
• Services / Not delivery related
• Consignment
• Miscellaneous Sales (Assets, RM’s, Leases, etc.)
• Returns
• Debit memo
• Credit Memo
• Rebate Settlement
• Special country / tax scenarios
Environment Favorable to Fraud

**Framework** for spotting high-risk situations

- **Perceived opportunity** (*I can do it / conceal it and not get caught*)
  - Poor internal controls
  - Lack of oversight

- **Incentive or Pressure** (*Financial or emotional force pushing to commit fraud*)
  - Meet expectations
  - Avoid criticism
  - Cover a mistake
  - Personal failures, needs

- **Rationalization** (*Personal justification for dishonest actions*)
  - Low compensation
  - Company is profitable

Framed Triangle
MIS 5121: Business Process, ERP Systems & Controls
Real World Control Failures: Adelphia Fraud
By: James Levan
Control Failure: Adelphia

• **Background:**
  - Adelphia was the 6th largest cable company in the U.S
  - The family that founded the company was using company funds for personal assets

• **Control Failures:**
  - Lack of segregation of duties- Rigas family controlled voting rights and made all company decisions
  - No system of checks and balances for company spending- used funds for pleasure purchases
  - The spending verification process was completed by members of the family
  - No accounting standards used- manipulated books for desired results

• **Results:**
  - The CEO, John Rigas is currently in jail facing criminal charges
  - Adelphia filed for bankruptcy and no longer provides cable to customers
  - Company is no longer listed on the New York Stock Exchange

• **What Could / Should those in Authority Have Done Different?:**
  - There should have been other people involved on the board of directors and in company decision making
  - Deloitte who audited Adelphia- should have been more thorough in its financial statement audit

• **Reference:**
  - http://www.wsj.com/articles/SB1027516262583067680
MIS 5121: Business Process, ERP Systems & Controls
Real World Control Failures:
By: Vinh Nguyen
Control Failure: Peregrine Systems

• **Background:**
  - CA based enterprise software company (founded in 1981) that specialized in change mgmt., IT service mgmt., and asset mgmt. software
  - Grew to a global company and at its peak in 2000, was valued at $3 billion and had 4500 employees
  - CEO – Stephen Gardner
  - CFO – Matthew Glass

• **Control Failures:**
  - Did not follow Generally Accepted Accounting Principles (GAAP)
    - Improper recording of revenue
    - Improper treatment of A/R
  - Failure to inform investors/stakeholders of Peregrine’s true financial situation
    - Lead to an artificially inflated stock price
  - Internal/External Audit failures
Control Failure: Peregrine Systems

• Results:
  - KPMG replaced Arthur Andersen and questions revenue sources (2002)
  - Filed for Chapter 11 Bankruptcy, 1400 employees laid off, and $4 billion in shareholder equity lost
  - Acquired by HP in 2005
  - CEO – sentenced to 8 years and CFO – sentenced to 5 ¼ years
  - Contributed to the need for Sarbanes-Oxley Act of 2002

• What Could / Should those in Authority Have Done Different?:
  - Governance – “Tone from the Top” – CEO and CFO gave go ahead for improper revenue recognition
    - Follow strict adherence to compliance laws (at the very least)
  - Increased involvement of Board of Directors
    - Communication between board of directors and CFO/Finance Lead should be open
  - Board only sessions/Audit Committee
    - Due diligence from internal and external auditors

• Reference:
  - [https://www.sec.gov/litigation/complaints/comp18205.htm](https://www.sec.gov/litigation/complaints/comp18205.htm)
MIS 5121: Business Process, ERP Systems & Controls
Real World Control Failures: Kingfisher Airlines | Vijay Mallya
By: DEVANG MEHTA
Control Failure: Inflated Valuations

- **Background: KINGFISHER AIRLINES | Vijay Mallya**
  - Defaulted on payments, salaries, taxes.
  - Multiple failure of Controls: Top Down / Banking / Government / who else?

- **Control Failures:**
  - Over Valuation of Assets when the company was making losses – Grant Thornton is the Auditor.
  - Single handed control of the entire enterprise.
  - No whistle blowing by the senior management,

- **Results:**
  - Vijay Mallya is currently in UK negotiating a settlement for restructuring.
  - Grant Thornton’s audit report under scrutiny.
  - Accumulated dues to the bank of $2 billion dollars, Accumulated loss

- **What Could / Should those in Authority Have Done Different?:**
  - A more transparent audit report by Grant Thornton
  - Proactive action by the banks, courts and the tax departments
  - Senior Management should have more control.

- **Reference:**
  - [http://www.businesstoday.in/topics/kingfisher-crisis](http://www.businesstoday.in/topics/kingfisher-crisis)
Control Failure: Inflated Valuation

- **Other Facts: KINGFISHER AIRLINES | Dr. Vijay Mallya**
  - Announced KFA was not in transportation business but in hospitality business
  - Personally chose the Air hostesses. Instructions were that passengers were to be treated as his own guests.
  - Launch was closer to his son Sid Mallya’s 18th birthday. Was a gift to him
  - Personally involved in Kingfisher Calendar Girls shooting.
  - Kingfisher Calendar Charts: Link

- [video](#)
MIS 5121: Business Process, ERP Systems & Controls
Real World Control Failures:
By: Jiehong Huang
Control Failure: Crazy Eddie

• **Background:**
  - Was an American retail business that sold electronic goods
  - Founded in 1971, Went public in 1984
  - Ceased operations in 1989
  - Family business, turned into the largest electronic chain in the New York metropolitan area

• **Control Failures:**
  - Crazy Eddie had been skimming cash for years
  - Inflated its stock price by adding imaginary stock and falsifying accounts
  - False financial statements propelled its stock to $79 a share from $8

• **Results:**
  - The Stock fraud caused company bankruptcy
  - A federal investigation showed that the company stole investors more than $145 million
  - Eddie Antar was arrested in Israel and two brothers were accused of a scheme

• **What Could / Should those in Authority Have Done Different?:**
  - Separation of operation and ownership
  - Hiring professional managers to run the business
  - Investors should request a third party to run an external audit when the company went public
Control Failure: Crazy Eddie

• **Reference:**
MIS 5121: Upcoming Events

• Reading Assignment 7 – *Due: Yesterday*
• Reading Assignment 8 – *Due: April 17*
• Reading Assignment 9 – *Due: April 24*

• Guest Lecture: Auditor’s Perspective - *April 18*

• Guest Lecture: SAP What’s New (HANA) - *April 25*
MIS 5121: Auditor’s Visit Topics

• _____
• _____
• _____
• _____
• _____
• _____
• _____
MIS 5121 : Auditor’s Topics 2015

• What are the general methodologies used for auditing?
• How do you classify risks?
• How do you review Segregation of Duties (modules vs. employees)?
• Have you personally detected a fraud scenario in your audit? If so, please explain
• How do you maintain your independence? Is that easy?
• What is your opinion on cyber-security laws being considered by the US government (CIA, CISA legislation)?
• How easy it is for an auditor to commit fraud?
• Does SAP provide good control environment vs. other systems (ERP, other)?
• Since SAP can be customized in so many ways, how does an auditor know what to audit when everything is different with each client?
System and Integration Controls
Key Information Technology Risks

- System Security
- Data Migration
- Data Interface
- Change Management
- Transport Security
- Instance Profile Security
- Table Security
- Data Dictionary, Program and Development Security
- Information Security Administration
- Logs and Traces
- Firefighter access
- Powerful User ID’s and Profiles
- Background Processing (Batch vs. foreground: real-time)
Table Security

- Tables are Integral part of SAP Application
  - Different Types of Data
    - System Tables (T000 – Clients, TDDAT – Table Authorization groups, USOBT_C – PFCG Transactions and Auth Objects)
    - Configuration / Control (T001 – Company codes, T001W – Plant Codes, TVAK – Sales Document Types)
    - Master Data (MARA – Material Codes, KNA1 – Customer Master: General)
    - Transaction Data (VBAK – Sales Doc Header, VBAP – Sales Doc Line Item, EKKO – Purchasing Doc Header)
  - Client-dependent and Client-independent

28,610+ Tables in SAP
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: Table Driven System Execution

- SAP Processing is customized using thousands of Configuration tables
  - Access via the ‘Implementation Guide’ (Transaction SPRO)
  - Entries determine how transactions are processed
  - Entries also support implementation of controls (e.g. processing parameters and limits)

- ERP Systems are Dynamic
  - Configuration table values and therefore system processing, are continually changed (process changes, business structure, etc.
  - Effective processing and control Requires:
    - Managed Design
    - Documentation
Table Security

- **Control Concerns**
  - Access to maintain / modify table entries
  - Authorization group assignment (esp. custom tables)
  - Logging of changes (certain critical tables only) – next section
Risk and Recommendation

Table Security

Risks:

- Many tables (e.g. config) control how programs function. Changing them equivalent to changing a program.
- Direct table changes bypass security, coded edit checks. High potential for corrupt data and compromise ‘un-alterability’. Changes to client-independent tables could have unexpected side affects (affects all clients).
- Users with update access to table entries can modify customized tables not assigned to specific authorization group.

Recommendations:

- Changes to configuration tables, table structures and certain system table entries should be made in DEV, tested in QA and migrated to PRD per change management process.
- Direct access to maintain tables restricted to very few individuals.
- Assure &SAP_EDIT backdoor change access in SE16N is Deactivated.
- All critical tables assigned to an Authorization Group to prevent users not part of that group from accessing them (even for ‘display’ only).
Risk / Control Matrix: Design Approach

- Define
- Drive
- Influence

Risks

Control Objectives

Control Activities / Controls

Control, system and Security Design + Implementation

- Automated Controls
- Manual Controls
- Application Security
- Segregation of Duties
- Approvals
- Reports
- Procedures

CONTROL DESIGN
Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables.
Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables.
Program & Development Security

- Types of Development Objects (FRICE)
  - **Forms** – outputs (invoices, Purchase orders, ...)
  - **Reports** – custom reports
  - **Interfaces** – SAP to other systems
  - **Conversions** – Data migration
  - **Enhancements** – Change system logic, use additional fields, etc.
    - User-Exits: defined SAP branches to custom code (lower risk)
    - Change SAP code (high risk, long term extra maintenance)
  - **Workflow** – non-config components, logic

- Development: custom programs
  - Typically ABAP (SAP SQL extension programming language)
ABAP can be a ‘black box’ – Control Concerns

– Unauthorized execution of Business Logic – bypassing security and SOD design.

– Unauthorized read access to business and configuration data – Could allow theft of critical data (e.g. credit card info) and be illegal

– Unauthorized modification of business and configuration data
  • Violate principal of change documents (Unalterable - not able to be changed or deleted)
  • Deletion of data can be illegal

– Repudiation of Business Process (denial of the truth or validity of something) – Legal requirements require non-repudiation regarding creation of and change to business transaction and master data.

– Identity Theft – Unauthorized access to customer master data could lead to identity theft and impact the data privacy and even criminal laws.

– Denial of Service – Auditors must communicate questionable findings to protect the investors and stakeholders and where violation is intentional criminal law is invoked.
Program & Development Security

- Is program code ‘good’
  - Does what it’s supposed to do
  - Limited to requirements only (not branch off to perform other nefarious actions)
  - Well-behaved: doesn’t mess up other programs, logic, operation of ERP system

- Good Development Practices
  - Clear, documented, approved requirements defined before coding
  - Define Requirements, Design Logic before major coding (e.g. use of function modules for common logic)
  - Peer Code Reviews
  - Experienced development leadership
  - Test, Test, retest **BEFORE** moving to PRD (strong change management governance)
Program & Development

- Other Control Concerns
  - Access to run ALL programs granted rarely and appropriately

- Secure Programs
  - ‘Authority Check’ inside the Code
  - Authorization Group assigned to program

- Development access (developers ‘key’) granted only in DEV
  - Programs unit tested in DEV, integration tested in QA and migrated to PRD per change management process

- Limit Development and Debug access in PRD
  - Debug access can provide unsecured view of tables
  - Debug access also can compromise ‘un-alterability’ via allowing deleting of table entries.
Risk and Recommendation
Program Security

Risks:

- Unintended, nefarious uses of program code
- Users capable of executing programs directly can compromise standard controls (access security, audit trails)
- Users with access to run ALL programs are allowed to run all executable programs (note not all programs are executed directly)
- Display access to ABAP code gives backdoor access to program execution
- Debug authority provides unsecured table viewing and table change

Recommendations:

- Active review, manage program code details
- Access to run programs restricted via SAP Security / Authorizations
- Further secure programs via assignment to authorization groups
- Basis Admin no Display access to ABAP code (prevent backdoor access)
- Debug authority restricted to effectively monitored ‘emergency users’
Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables.

- **IT / Security**
  - Security Configuration
  - Automated (Access) Control

- **Risk / Control Matrix**
  - Subset

- **Security Analysis Tool**
  - Segregation of Duties
  - SOD Controls & Sensitive Access

- **Program Development**
  - Functional Spec
  - Technical Specification
  - Automated (Custom) & Manual Controls

- **SOX Section 404 Integration**

- **Business Process Teams**
  - Bus Process Reqmts
  - Training & Procedures
  - Manual Controls

- **GRC**
  - Risk / Control Matrix
  - Automated: Standard & Configuration
Data Dictionary Security

- Central Catalogue of:
  - Data definitions and descriptions
  - Relationships between data elements / structures
  - Relationships between data and use in programs and screens

- Control Concerns:
  - Data Dictionary changes could affect the data integrity in system
  - Access to make changes needs to be restricted to appropriate individuals
  - S_DEVELOP Authorization object controls access to create / maintain / delete APAP dictionary & repository objects

- Also called ABAP/4 Dictionary in SAP
Risk and Recommendation
Data Dictionary

Risks:
- PRD Access to S_DEVELOP Allows direct changes to Data Dictionary which could compromise integrity of the data
- Any Data Dictionary change could compromise integrity of the data

Recommendations:
- No one (including Basis Administrators) should have update access to Data Dictionary in Production (PRD)
- Changes to data dictionary performed in DEV, tested in QA and migrated to PRD per change management process
- Developer access restricted appropriately using SAP Security/authorization concept
Information Security Administration

- Security Administration can be:
  - Centralized
  - Decentralized
  - Hybrid of both

- Control Concerns:
  - Segregate:
    - Role Development
    - User Administration (Assign Roles, change).
  - Do not Develop / Change Roles directly in PRD
    - Develop and unit tested in DEV, integration tested in QA and migrated to PRD per change management process
**Risk and Recommendation**

Information Security Administration

**Risks:**
- If User Administration access is not limited, higher risk of unauthorized and excessive access in SAP
- No Segregation of User Administration tasks, higher risk of inaccurate or unauthorized access assigned to users and profiles in SAP

**Recommendations:**
- Define Owners of all SAP systems, clients and data or Processes
- System and Client Owners responsible for:
  - Approving all changes to their systems / clients
  - Authorizing overall access to the system
- Data / Process Owners responsible for:
  - Control of overall data / process components in the systems / clients
  - Authorizing specific access to data / processes within the PRD system
- Same people do not have access to create, maintain and assign roles
- Role Creation or maintenance not performed in PRD environment
System Logs and Traces

- Need to be activated to exist
- **System Audit Log** can be set up (SM19) to record:
  - Successful / unsuccessful Dialog logon attempts
  - Successful / unsuccessful RFC logon attempts
  - RFC calls to function modules
  - Changes to user master records
  - Successful / unsuccessful Transaction starts
  - Changes to the audit configuration

- **System traces** (ST01 / ST05) for:
  - Database access
  - ABAP/4 programs
  - Internal system activity
  - Developer traces
  - RFC Calls
SAP Integrated Change Log

- Built into most system documents (e.g. Sales Order, PO, Delivery, ...)

- Configuration to turn on/off some changes

- Data Stored in tables – available for subsequent reporting

- ‘Big Brother’ is watching?

- Excellent for problem diagnosis
Risks:
- If audit files (Logs and traces) are not secured at the operating system level for each application server, they could be maliciously deleted.

Recommendations:
- Secure folders where log and traces files are stored at the operating system level.
- Develop and use procedures for how to review and run traces at part of routine system security monitoring.
Table Logging

- In addition to system change logs supports traceability
- Needs to be activated in system to exist
- Can be activated individually by table via SE13
  - Concern: for high change rate tables logs fill up fast
Key IT Controls Overview

• Table, Security Administration
  – 2-3 risks that exist
  – Common control recommendations for each

• Program, Development, Data Dictionary
  – 2-3 risks that exist
  – Common control recommendations for each
Assignment Questions

• How common are missing or faulty authorization checks?
• **Explain the difference between the IT general application controls and the IT general controls.**
• Is it possible for a fraudulent user to make a copy of the logs and reinstall them into the system in order to delete the originals to hide a fraudulent act, or would there be a “protected” log system that would still record this activity?
• What is the importance of the principle of inalterability?
• According to the principle of unalterability, some certain fields won’t allow to be changed. What should the staff do if an emergency is happening and he needs to make the change to the document?
• *Since we can change documents in SAP, so how we change the posting date in SAP if we forget to select date and SAP set it as a default date?*
• *What tools allow a company to easily monitor, capture and review logs?*
• When the cost of implementing a compliance control is higher then the benefit obtained, what must an organization do to ensure efficiency and profitability?
SAP Environment Security Components

- Network Security
- Workstation Security
- Operating System Security
- Database Security
- SAP Application Security
Assignment Questions

• How much automated controls should be desired? Is it beneficial to consider controls at design phase or are controls introduced as and when needs arise?

• Who in a company is primarily responsible for the identification and monitoring of SAP related control?

• What kind of vulnerabilities are associated with RFC communication?

• Could you please explain how to segregate the duties related to application control?

• Who generally has the access to debug activities and how does it work?

• Debugging is risk area but is critical for application support and maintenance. What controls are most relevant in real life scenario?

• What should be done in the case logs are deleted and they cannot be retrieved?

• For my understanding, application only works on system generated/ recurring transaction data. For manually post data, is only control to perform an audit?

• How does the abuse of the principle of least privilege for the individual Basis authorizations represent as a high risk for the availability of SAP system and for the integrity and consistency of the data and the processing logic?
Assignment Questions

• If a business catastrophe like Cantor Fitzgerald on 9/11 happened today, how would the company protect its data, and who would access it in an emergency assuming that corporate leadership, or those normally authorized were incapacitated or deceased?

• What are in common between external document number assignment and internal document number assignment?

• What application control do you think is the best? To me, I believe it is the logging features, although they most likely aren’t used as much as they should be.
Break Time
Risk / Control Matrix
Final Exercise
Risk / Control Matrix: Design Approach

- Define
- Drive
- Influence

- Risk
- Control
- Objectives
- Control Activities / Controls

Control, system and Security Design + Implementation

- Automated Controls
- Manual Controls
- Application Security
- Segregation of Duties
- Approvals
- Reports
- Procedures

CONTROL DESIGN
Risk / Control Matrix: Final Exercise

• Agenda

  – Last Class (April 4): Part 1 - Identify Risks
  
  – This Class (April 11): Part 2, 3
    • Risk Priority (Severity & Likelihood)
    • Identify Controls
    • Link Controls to Risks

  – April 18: Part 4 - Complete Control Definitions
  
  – April 25: Part 5, 6 - Control Process / Audit Details; Personal Questions

  – Due April 28 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
Risk Assessment

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Considerable Management Required</td>
<td>Extensive Management Essential</td>
</tr>
<tr>
<td>High</td>
<td>Management Effort Required</td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Risks may be worth accepting with monitoring</td>
<td>Management Effort Worth While</td>
</tr>
<tr>
<td>Moderate</td>
<td>Accept and Monitor Risks</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Acceptable Risks</td>
<td>Manage &amp; Monitor Risks</td>
</tr>
<tr>
<td>Low</td>
<td>Accept and Monitor Risks</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk / Control Matrix: Final Exercise

Part 2: Identify key controls for the Order to Cash (OTC) process at GBI

- Tab: Part 2 – GBI Controls
- Identify at minimum 15 controls for the process
- Identify a minimum 3 controls 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
- At least two (2) controls must be Automated / Config controls
Part 3: Link Risks (Part 1) to the Controls (Part 2)

- Tab: Part 1 – GBI Risks
- At least one (1) control must be identified for each risk identified as High Severity or High Likelihood / Frequency
- A given control may address multiple risks (listed once in Part 2 tab and multiple times in Part 1 tab)
- A given risk may be addressed by multiple controls (listed once in Part 1 tab and multiple times in Part 2 tab)
- Risks without out a control:
  - Acceptable Risk: Business agrees no controls will be developed
  - TBD (To Be Determined)
Extra Slides
Extra Slides

```
<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

```

```
<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
<td>High</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).
SAP System Characteristics
Integrated Database

- All transactions stored in one common database in thousands of tables
- Module automatically create entries in other modules (e.g. OTC creates financial postings)
- Auditors need to understand the flow of information
- Databases can be accessed by any module
- Users view the system as Transactions, documents and reports
- SAP modules are transparent to users
Technical Complexity

- System usually resides on multiple computers
  - Using different servers and databases
  - Coordination is a challenge
- Legacy systems may be interfaces
- Distributed systems and bolt-ons contribute to complexity
  - A
  - B
Processing

Transactions processed by the system initiate new transactions and postings automatically (event driven)

If initiating transaction is invalid, inaccurate or incomplete that can have significant impact on the organization

- Suggests needs for preventative controls rather than detective controls

Data entry accuracy improved through use of default values, cross-field checking and alternate views into the data

SAP uses online real-time processing

- Traditional ‘batch’ controls / processing and audit trails are no longer available
- Period closing will be different in SAP
COSO Framework (2013)
COSO Framework (2013)
Codification of 17 principles embedded in the original Framework

**Control Environment**
1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

**Risk Assessment**
6. Specifies relevant objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

**Control Activities**
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

**Information & Communication**
13. Uses relevant information
14. Communicates internally
15. Communicates externally

**Monitoring Activities**
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies
Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables.
Controls: Integration Points

Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables.

Program Development

Functional Specification

Technical Specification

Automated (Custom) & Manual Controls

Automated (Access) Control

SOX Section 404 Integration

Automated: Standard & Configuration

Business Process Teams

Segregation of Duties

Security Analysis Tool

SOD Controls & Sensitive Access

GRC

Risk, Control, Configuration, and Manual Controls (GRC)

Risk/Control Matrix

Automated: Standard & Configuration
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 and other exercises. (Optional) Details will be announced via a blog post in last couple weeks of class.