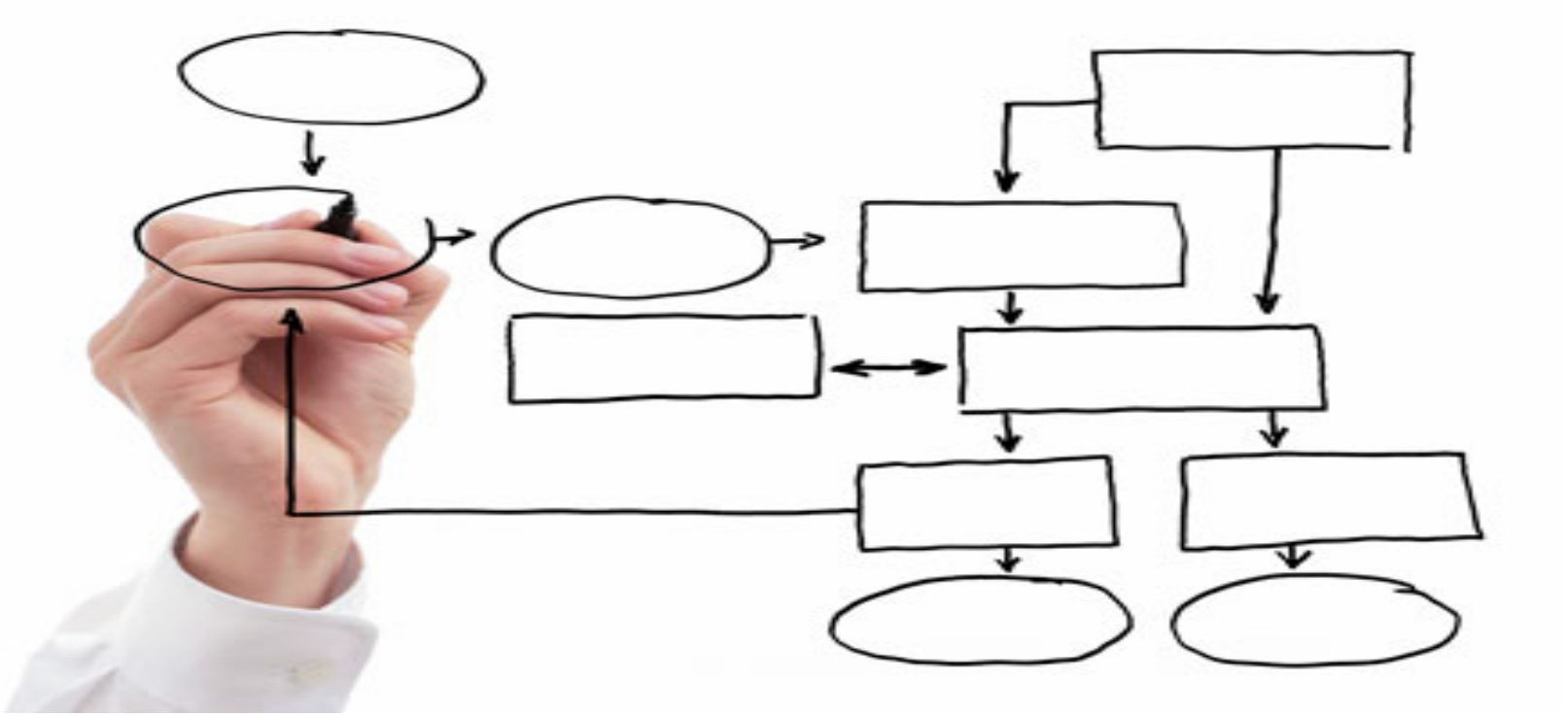


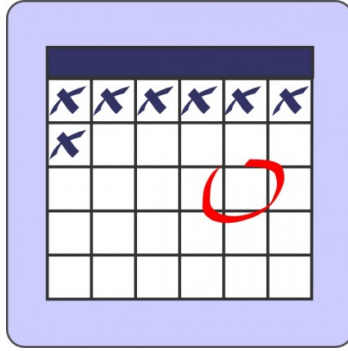
MIS 5121: Enterprise Resource Planning Systems

Week 12: *System and Integration Controls*

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

MIS 5121: Upcoming Events



- Reading Assignment 8 – *Past Due: April 12*
- Reading Assignment 9 – *Due: April 19 (Week Earlier)*

- Extra Credit Opportunity (Optional) - *Due: April 28*
- Final Exercise (Risk/Control Matrix) – *Due: April 30*

- **Exam 3** – In class*: May 4*

Control Failure: Ibtissam Bazzine

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

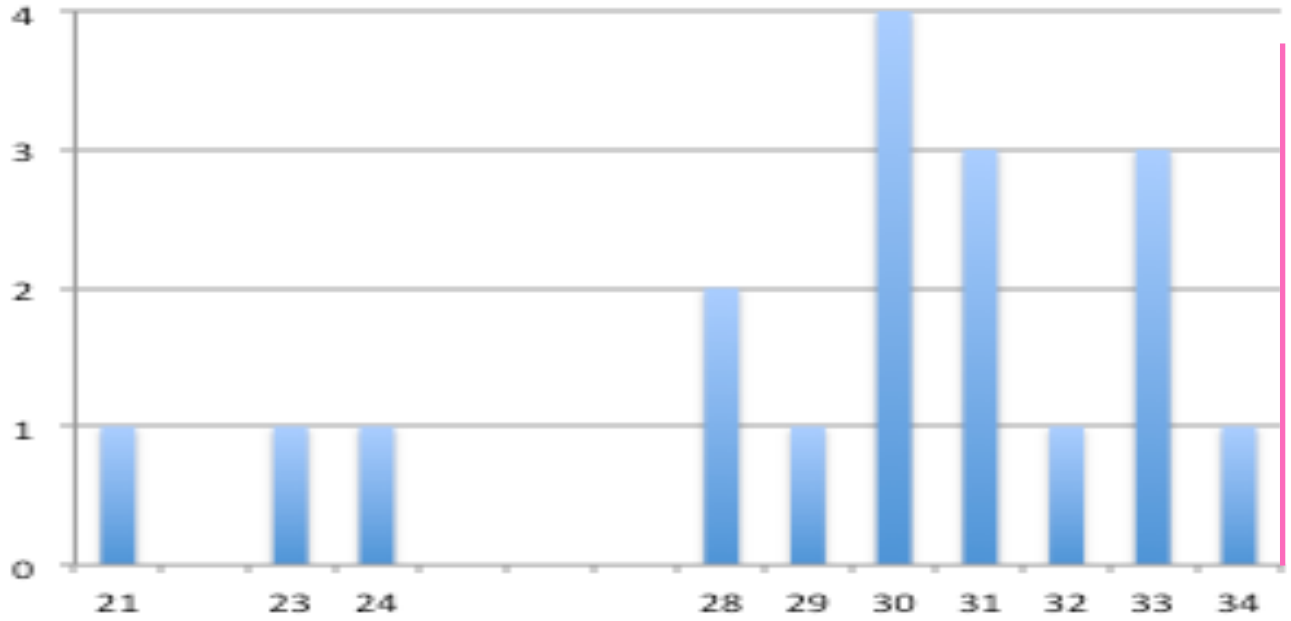
Control Failure: Pavel Sasna's Presentation

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

Control Failure: Michael Roth's Presentation

- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

Exam 2: Results

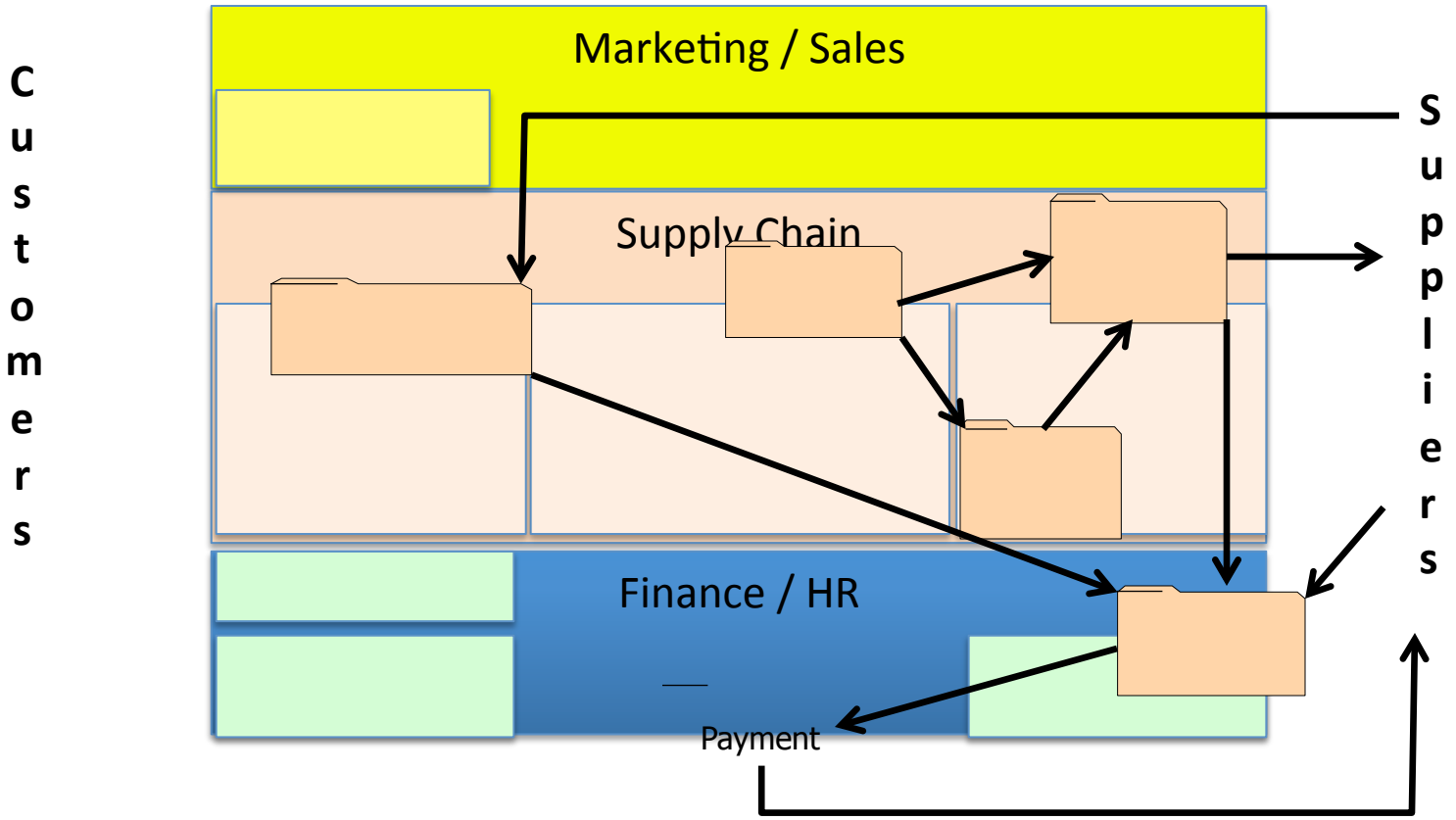


- One question ‘bad’ (My answer may be correct in broader context)
- Results will be ‘curved’ to score of 34 vs. perfect score of 36

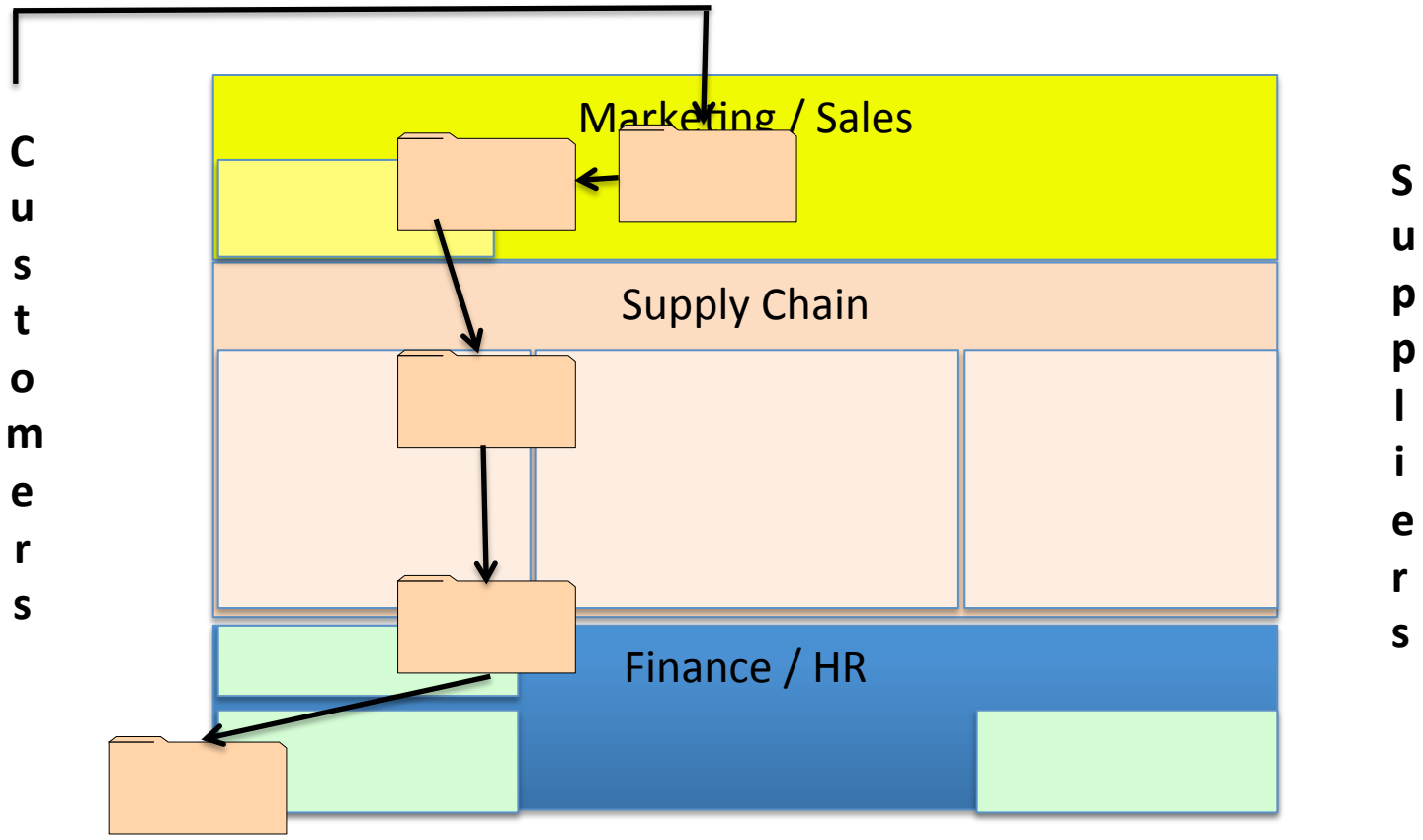
Exam 2: Actions

- **Quick Review of 'key' concepts, Lessons (Final week of class – April 27)**
  - **Not reteach, just review**
  - **Will be included in Exam 3**
- Will Distribute Review sheets
  - Outline, Illustrations only: you can annotate (examples next 3 slides)
  - Allowed to have the review sheets with you while taking Exam 3

Procurement at GBI



Order to Cash at GBI



Order to Cash

- Common Risks
  -
  -
  -
  -
  -
  -
  -
- Common Controls
  -
  -
  -
  -
  -
  -
  -

System and Integration Controls

Key Information Technology Risks

- **System Security**
- Information Security Administration
- Logs and Traces
- Powerful User ID's and Profiles
- **Instance Profile Security**
- **Change Management**
- **Transport Security**
- **Change Control**
- **Data Migration**
- **Data Interface**
- Table Security
- Data Dictionary, Program and Development Security
- Firefighter access

SAP: Table Driven System

- Tables determine how transactions are processed and controls are implemented
- Table values establish processing parameters and limits
- SAP is customized using thousands of tables through the implementation guide (SPRO)

- Table values and therefore system processing, are continually changed

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

Client Dependent vs. Independent

System/Instance

Client Dependent

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

Client Independent

- **Programs (ABAP)** **> Repository Objects (Client Independent Config**
- **Data Dictionary** **- Currency, UOM's**
- **Parameters** **- Pricing Tables**
- **Authorization Objects** **> Transactions**

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 Deactivatd
- All critical tables assigned to an Authorization Group to prevent users not part of that group from accessing them (even for 'display' only)

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)

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
  - Design 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

- Control Concerns
  - Access to run ALL programs granted 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

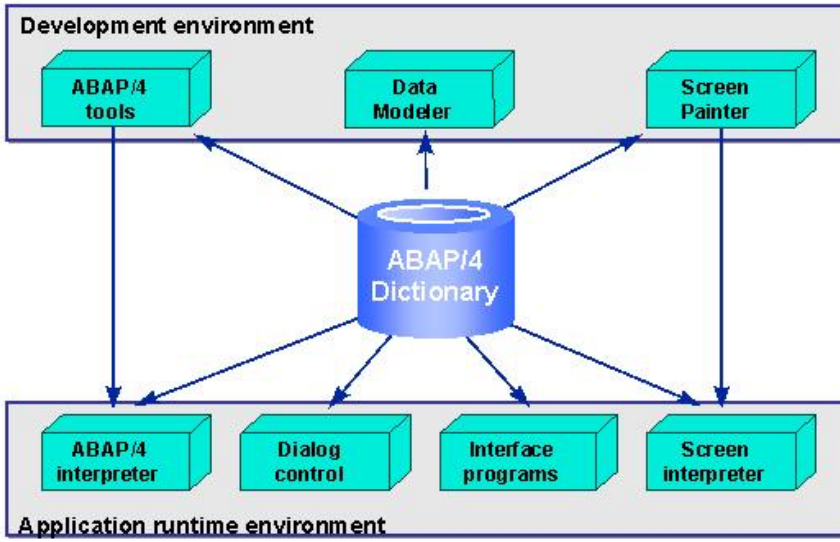
Risks:

- 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 provides backdoor access to program execution
- Debug authority provides unsecured table viewing and table change

Recommendations:

- Access to run programs restricted via SAP Security / Authorizations
- Further secure programs via assignment to authorization groups
- Basis Administrators not given on-going Display access to ABAP code (prevent backdoor access)
- Debug authority restricted to effectively monitored ‘emergency users’

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 acccess 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

Risk and Recommendation
System Logs and Trace Files

Risks:

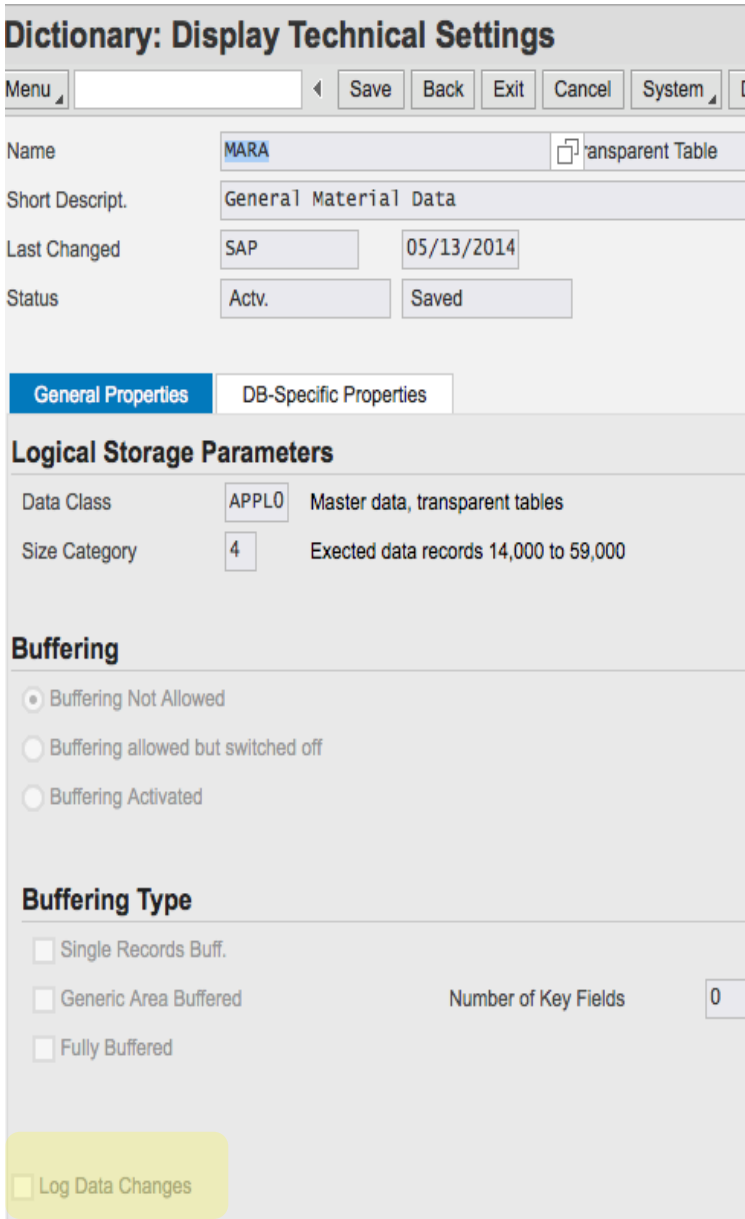
- If audit files (Logs and traces) are not secured at the operating system level for each application server, they could be maliciously deleted

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

- ABAP code was referred to as Black Box. Does that mean it was dangerous or it was the only reliable form of evidence in a business tragedy / issue.

- Who can control the “debugging’ feature? How can it be use to violate the principle of un-alterability?

- Can you please explain the synchronous and asynchronous processing?

- Risk during updates: How do SAP prevent shutdown of the entire system caused by an update error, especially businesses with offices globally?

- What are some pros/cons of relying on an external consultant for ERP solutions, rather than employing a full time employee for this position?

- **Do you find the strictness of the controls in SAP to be overkill, or do you think you are sacrificing any efficiency? How would you weigh the need have efficiency with the need to have things like un-alterablity?**

Assignment Questions

- Can SAP still be hacked from a disgruntled employee at SAP? or does SAP belong to the owner (on licensing) and all SAP users are deactivated?

- *What is the difference between general application and IT general controls?*

- Do you find the strictness of the controls in SAP to be overkill, or do you think you are sacrificing any efficiency? How would you weigh the need have efficiency with the need to have things like un-alterablity?

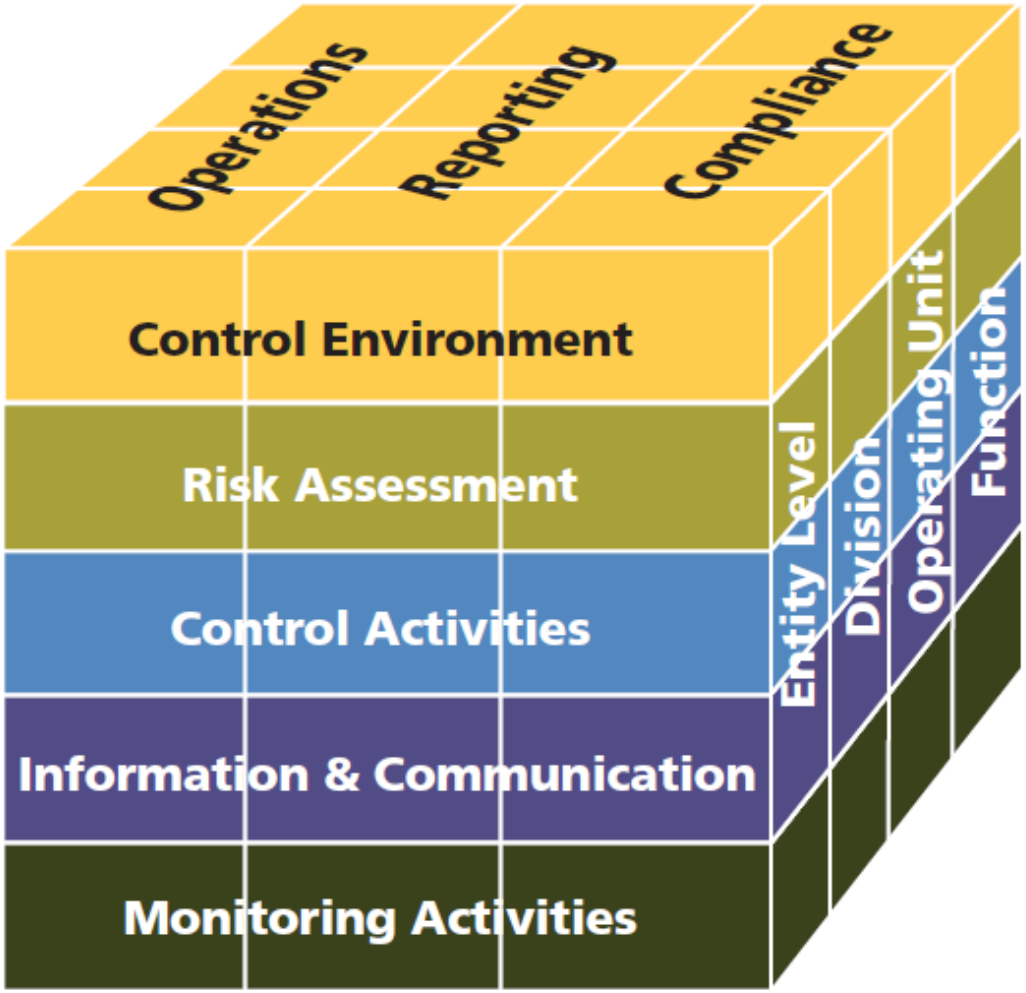
- When we first touch the SAP I remember that once we enter information to SAP it is very hard to delete, what kinds of document that can be deleted and that cannot?

- To ensure identity authentication, different users are assigned with unique user IDs. My question: in terms of 'Unique', are user IDs only unique in a specific company or are they unique around the world?

Break Time

Risk / Control Matrix
Final Exercise

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

Risk / Control Matrix: Final Exercise

- Agenda
  - Last Class *(April 6)*: Part 1 (Identify Risks)
  - This 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 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

Risk / Control Matrix: Final Exercise

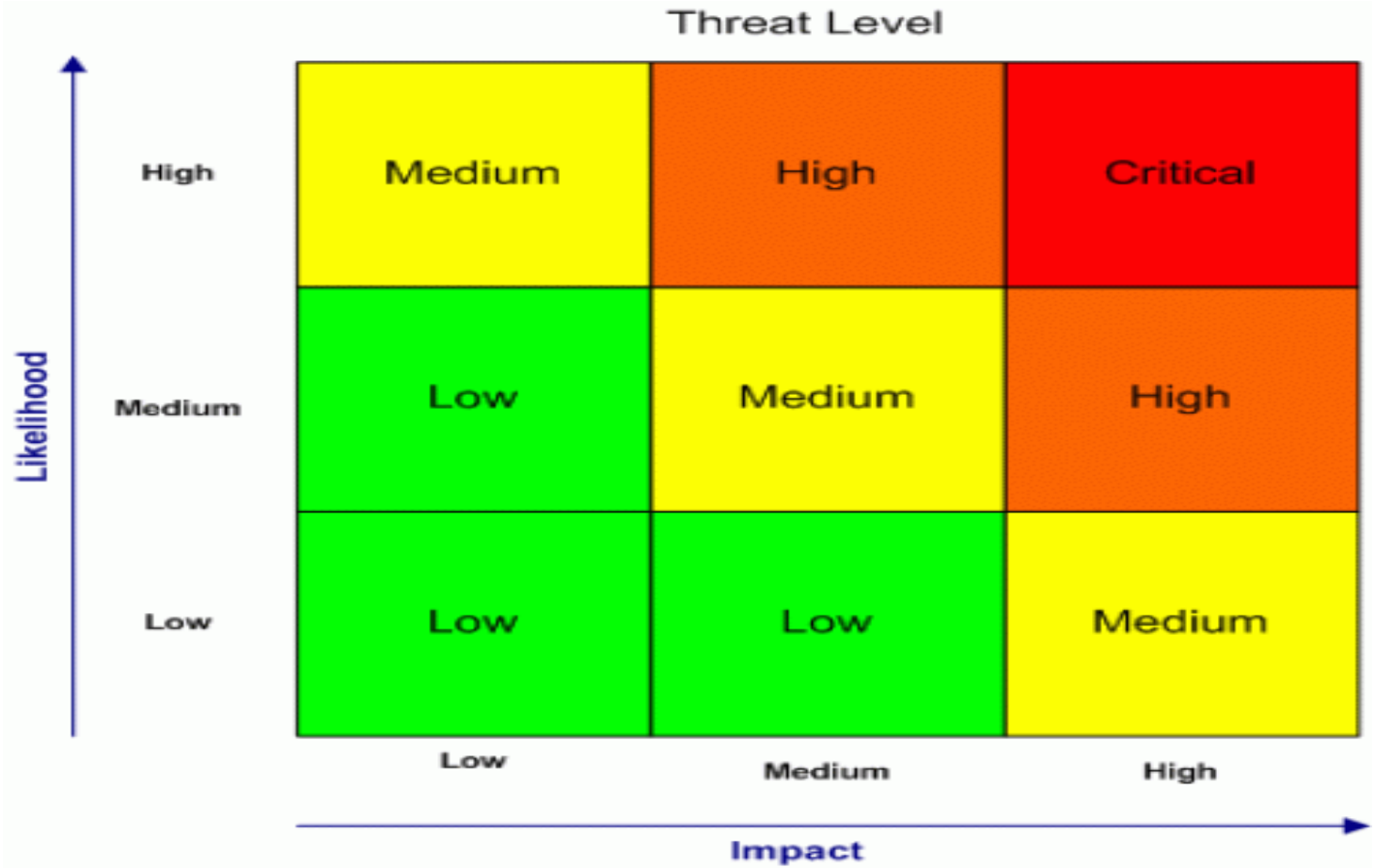
Part 3: Link Risks (Part 1) to the Controls (Part 2)

- 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)

Risk Assessment

Extra Slides

Extra Slides



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

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