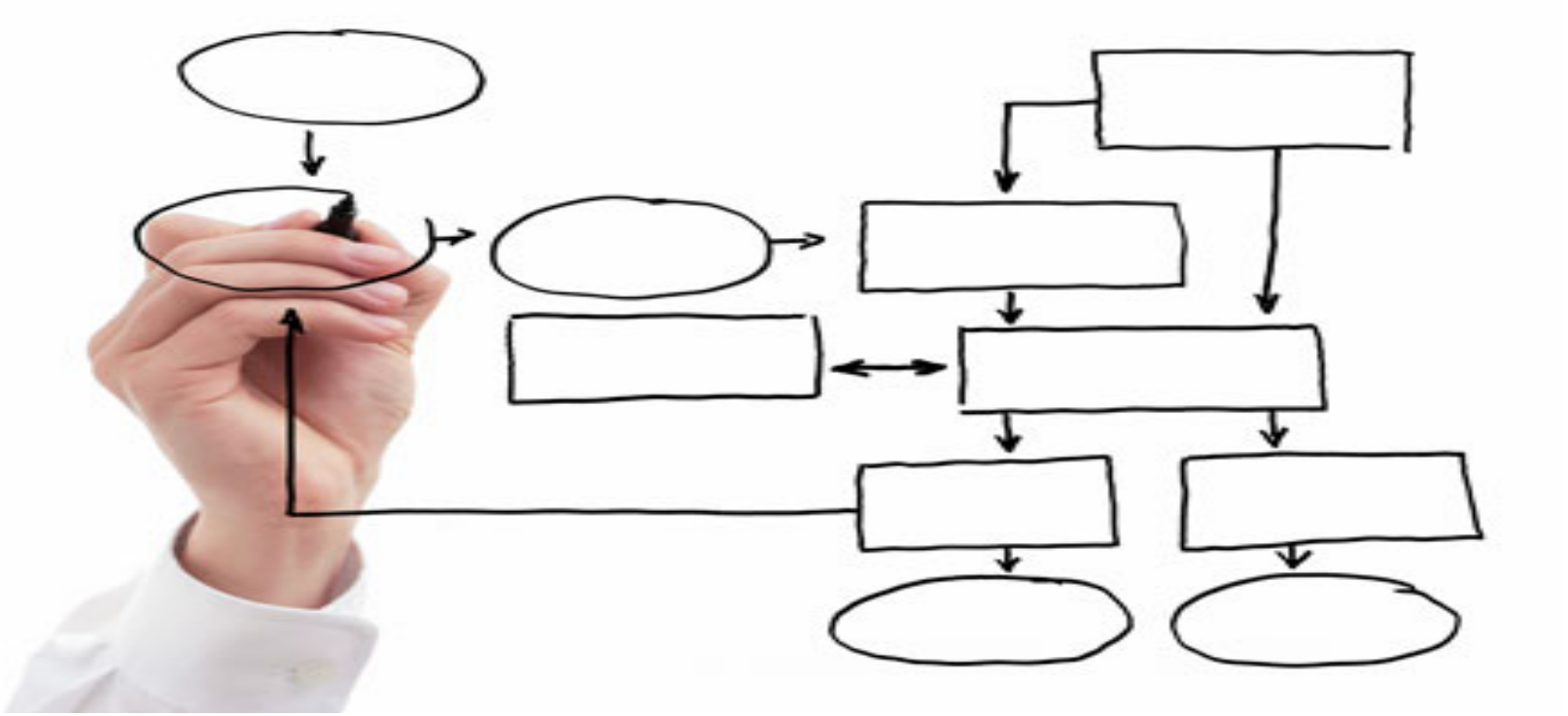


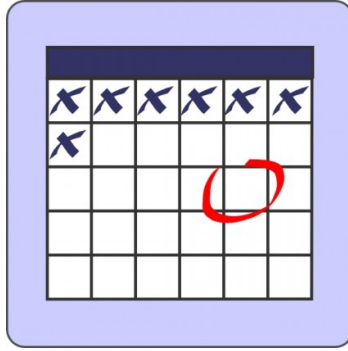
MIS 5121: Enterprise Resource Planning Systems

Week 14: *Misc Topics, Review, Q&A*

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

MIS 5121: Upcoming Events



- *April 27 Class*: Review and Exam Guide,
  Your Q&A Few loose ends

- Extra Credit Opportunity (Optional) - *Due: April 28*

- Final Exercise (Risk/Control Matrix) – *Due: April 30*

- Last I'll accept overdue Assignments– *May 3 11:59 pm*

- **Exam 3** – In class*: May 4*
  (Potential conflict with Capstone Class Resolved)

Control Failure: Kevin Mcginn

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

Control Failure: Paul Thomas's Presentation

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

Control Failure: Lucia Okaro's Presentation

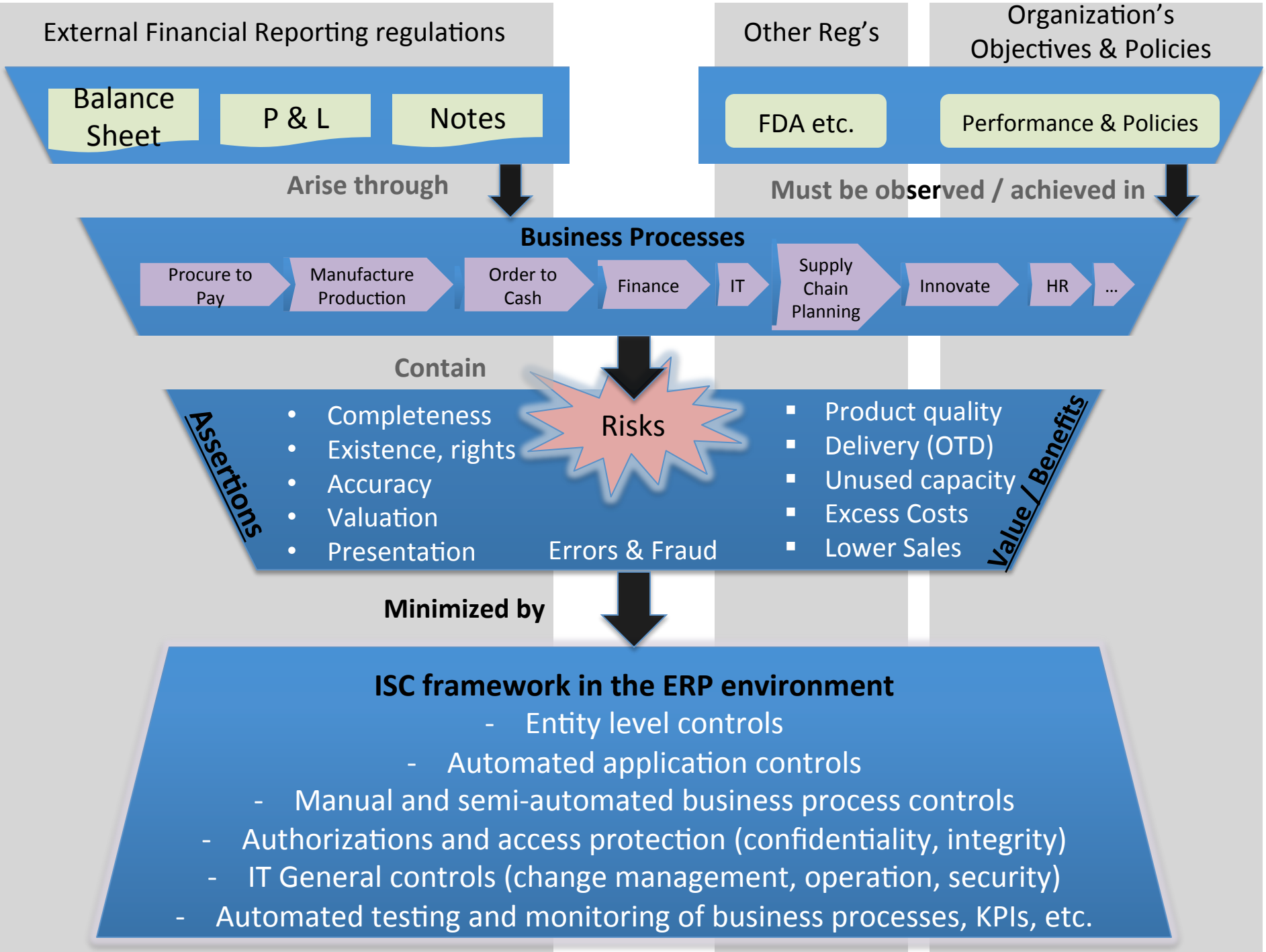
- Background:
  - ❖
  - ❖
- Control Failures: 2006 – 2009
  - ❖
  - ❖
- Results:
  - ❖
  - ❖
- Reference:
  - ❖

Review: Key topics to remember
(i.e. may be on a future test)

Exam 2: Actions

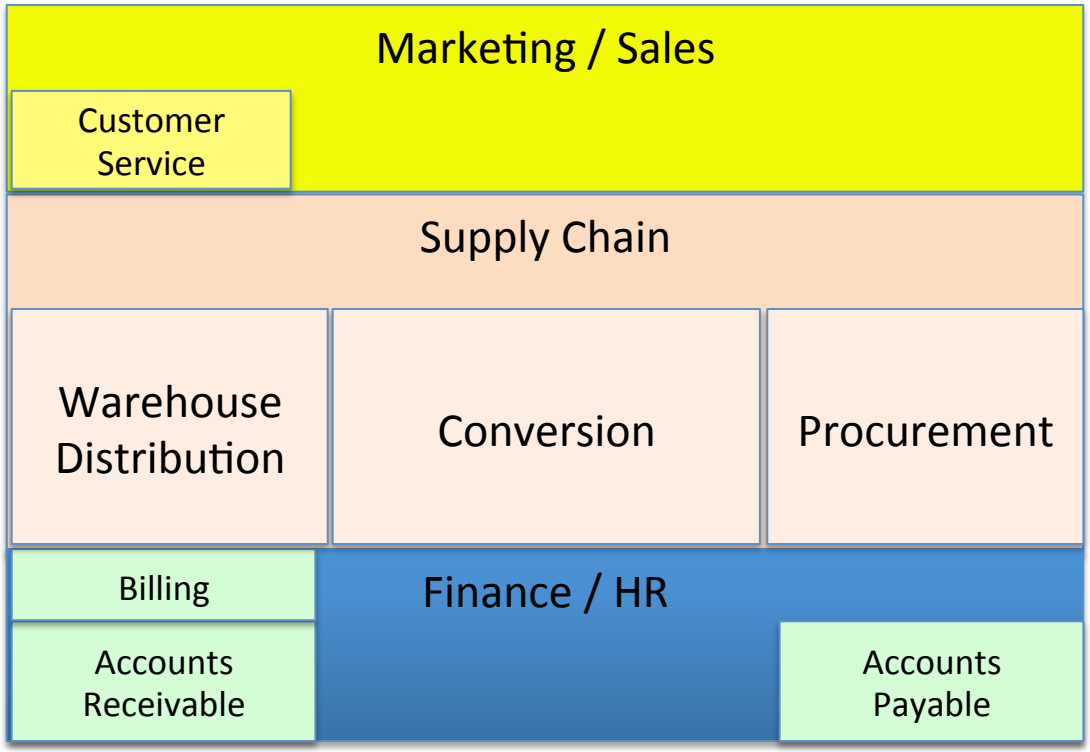
- **Quick Review of 'key' concepts, Lessons Not reteach, just review**
  - **Not reteach, just review**
  - **Could be included in Exam 3**

- Review sheets
  - Outline, Illustrations only: you can annotate (examples next 3 slides)
  - Allowed to have **up to 3 pages** of the review sheets with you while taking Exam 3


External Financial Reporting regulations
Other Reg's
Organization's Objectives & Policies
Balance Sheet
P & L
Notes
FDA etc.
Performance & Policies
Arise through
Must be observed / achieved in
Business Processes
Procure to Pay
Manufacture Production
Order to Cash
Finance
IT
Supply Chain Planning
Innovate
HR
...
Contain
Assertions
Completeness
Existence, rights
Accuracy
Valuation
Presentation
Risks
Errors & Fraud
Product quality
Delivery (OTD)
Unused capacity
Excess Costs
Lower Sales
Value / Benefits
Minimized by
ISC framework in the ERP environment
- Entity level controls
- Automated application controls
- Manual and semi-automated business process controls
- Authorizations and access protection (confidentiality, integrity)
- IT General controls (change management, operation, security)
- Automated testing and monitoring of business processes, KPIs, etc.

Global Bike Organization

Customers



Suppliers

Business Process Vs. Function

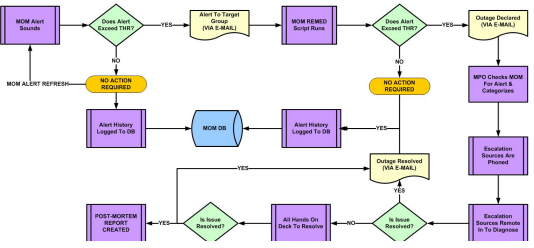
Function

‘An operation / group who perform related tasks routinely to carry out a part of the mission of an organization..’

Business Dictionary

Process

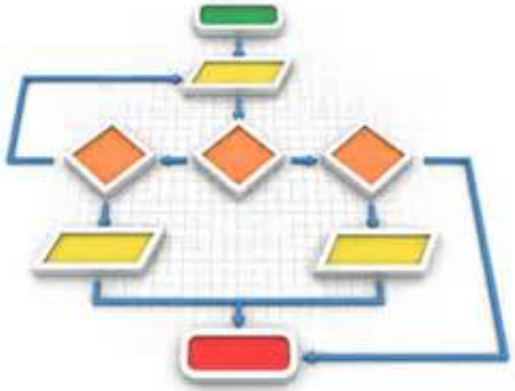
‘A series of logically related activities / tasks performed together to produce a defined set of results.’



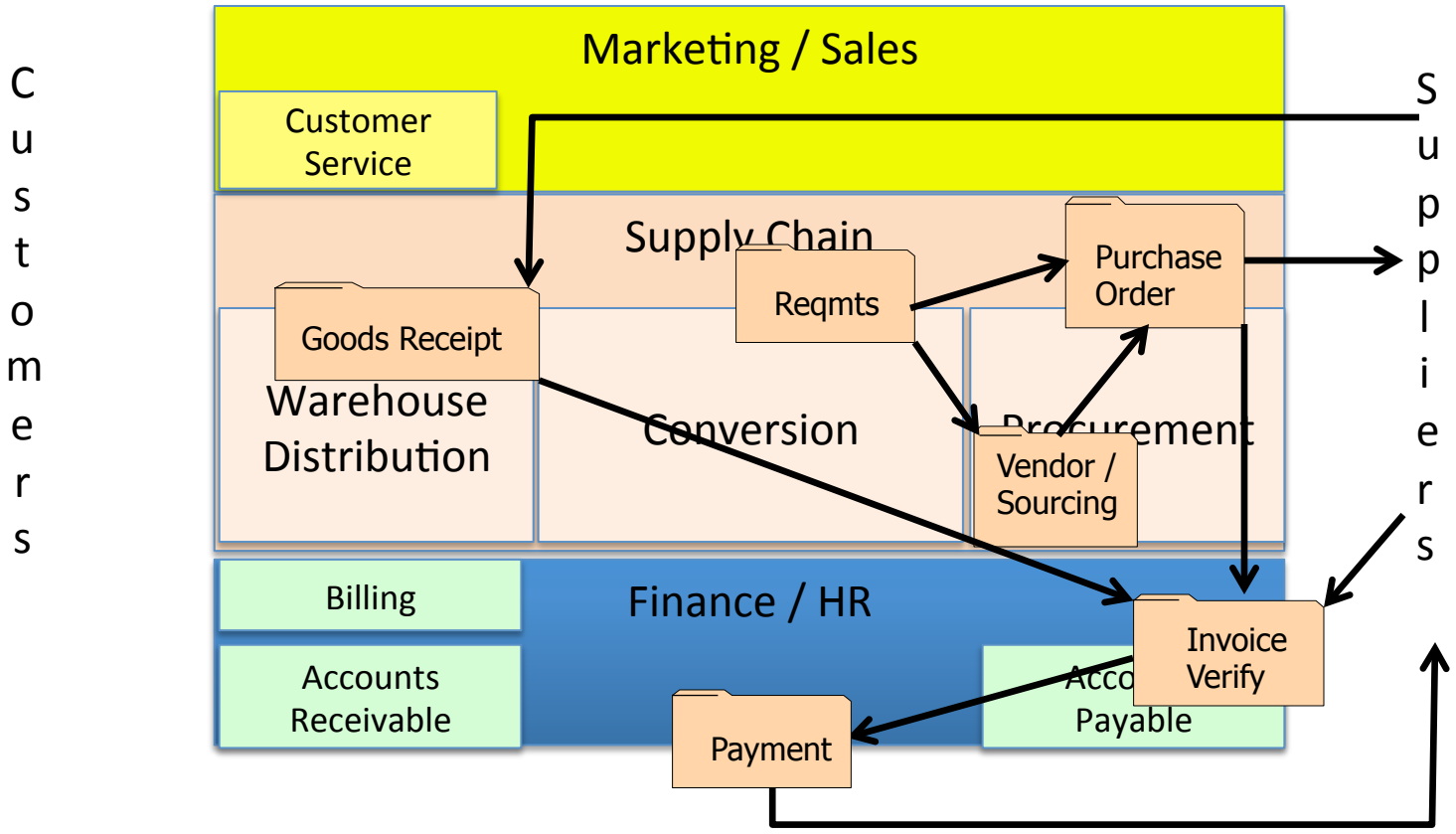
Business Dictionary

Business Processes

- Sales
- Order to Cash
- Procurement to Pay
- Supply Chain Planning
- Manufacturing / Production
- Innovate / Commercialize
- People / Human Resources
- Finance / Record and Report



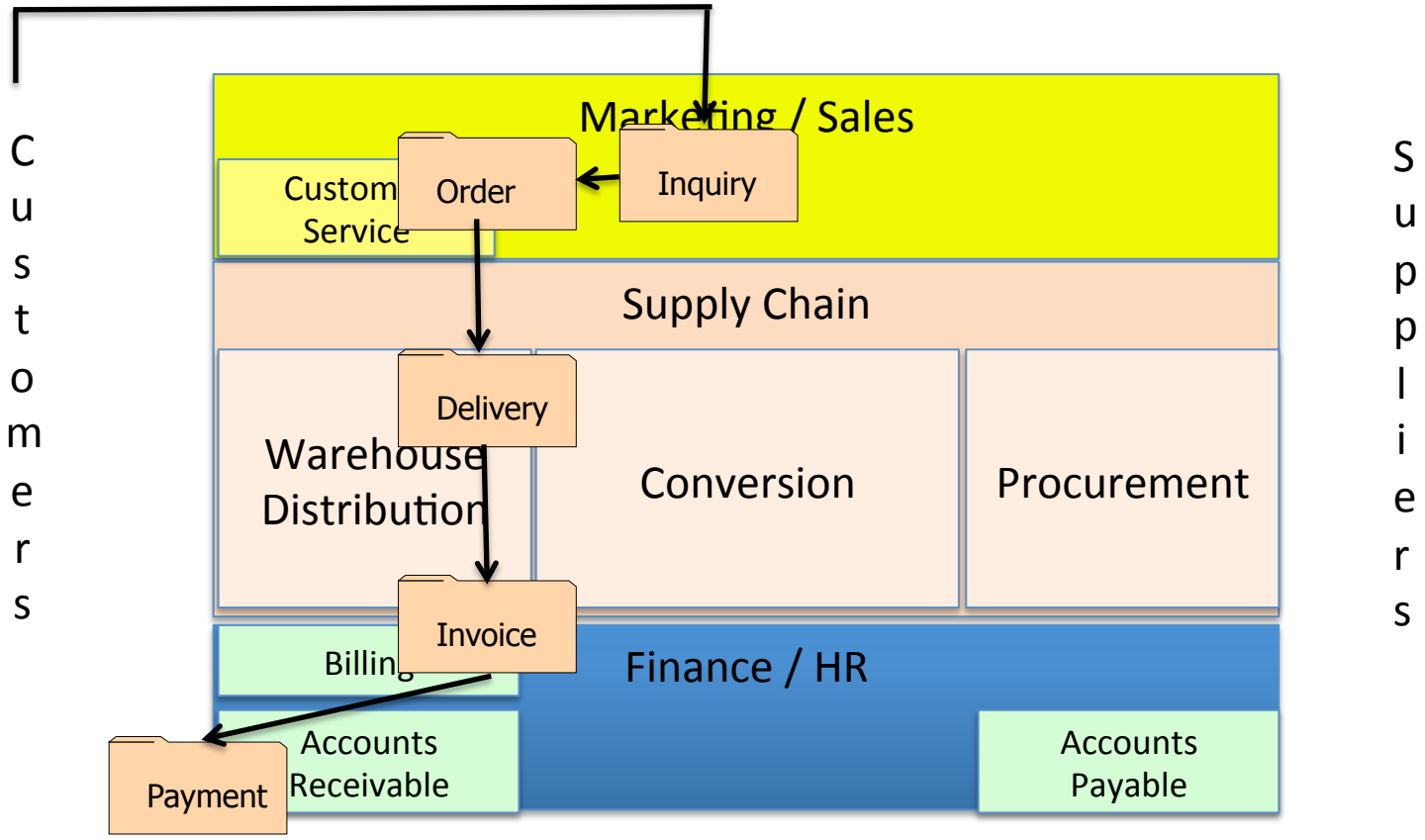
Procurement at GBI



Risks / Controls

- **All** slides, discussions content related to Risks and related controls
  - No need to memorize every example
  - Understand what is a risk vs. what is a control
  - Do remember a few examples of risks **and** controls in each area discussed
    - Procure to Pay Process
    - Order to Cash Process
    - Financial Processes
    - Inventory

Order to Cash at GBI



Assertion

Definition

‘a confident and forceful statement of fact or belief’

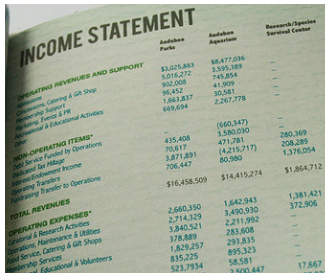
Oxford Dictionaries

In Auditing: ‘what management claims’

Management Assertions

Taxonomy for class

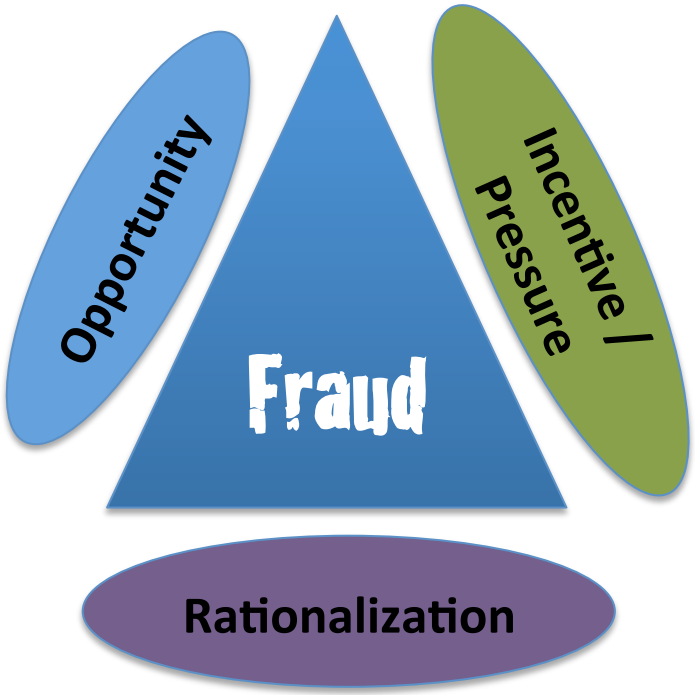
- Occurrence / Existence (timing)
- Completeness
- Accuracy / Valuation
- Rights (Ownership)
- Summarization / Presentation



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



Fraud Triangle

Inventory: Quantities

Inventory Record Accuracy: Does Physical inventory match system records

- Material / Batch
- Quantity
- Location

Method: Physical Counting

- Periodic (e.g. yearly, quarterly, …) Frequency can depend on risk (e.g. value)
- Complete Count?
- If ‘miss’ someone else Adjusts Records based on Count

Inventory: Quantities

Inventory Record Accuracy: Does Physical inventory match system records

Methods: Cycle Counting

- **Continuous** counting of sections of inventory
- Hit or Miss based on tolerances (e.g. zero for package, +/- for bulk)
- If 'miss' someone else Adjusts Records based on Count
- Root cause analysis of reason and correction for 'miss'
- Track IRA % (# Hits / # checks)
- Acceptable alternative for full physical counts

Common Issue: timing of physical moves vs. system recording

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

Client Dependent vs. Independent

System/Instance

Client Dependent

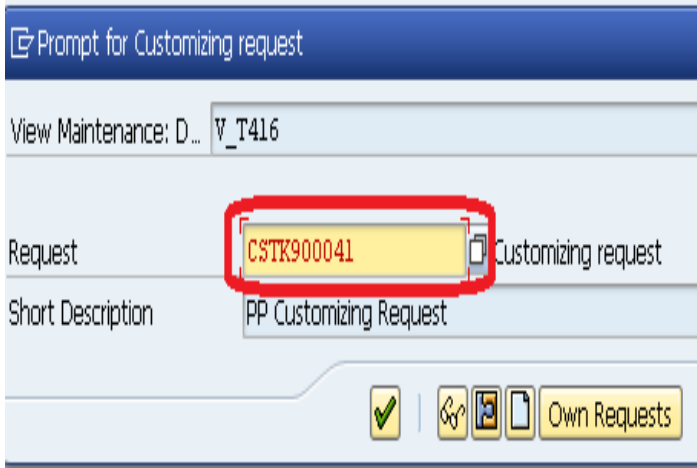
Dev 100 Master (Gold)	Dev 110 Dev Test	Dev 180 Data Conversion	Dev 900 Sandbox
- Master Data - Transaction Data - User Management / Data	- Master Data - Transaction Data - User Management / Data	- Master Data - Transaction Data - User Management / Data	- Master Data - Transaction Data - User Management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

Client Independent

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

SAP Change Management

- Transport (the truck icon): contains the changes (including role changes) moved from client to client and system to system per transport path
- 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



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

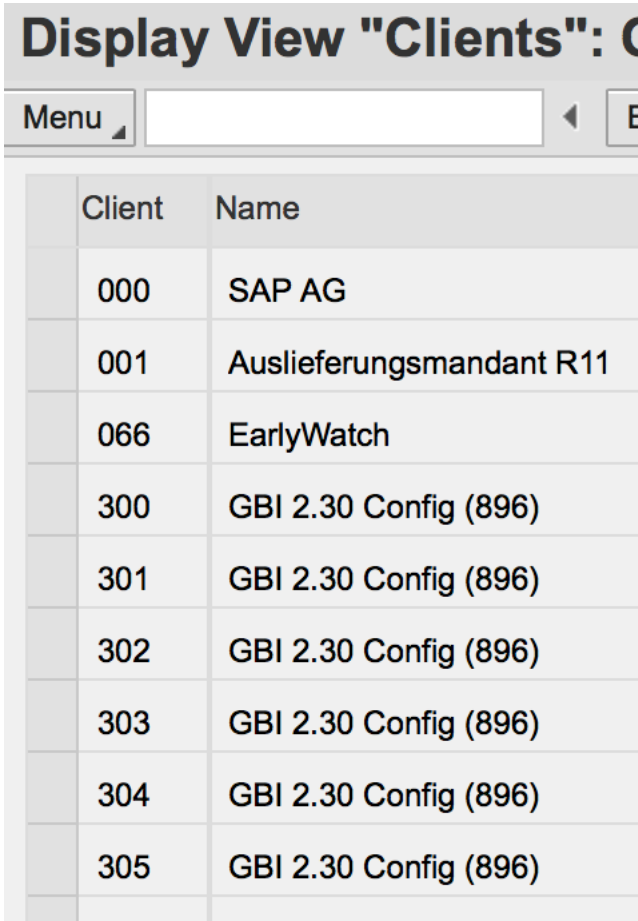


Table Security

- Tables are Integral part of SAP Application
  - Different Types of Tables
    - _____
    - _____
    - _____
    - _____

- SAP is customized using thousands of _____ tables through the _____ (SPRO)

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)

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

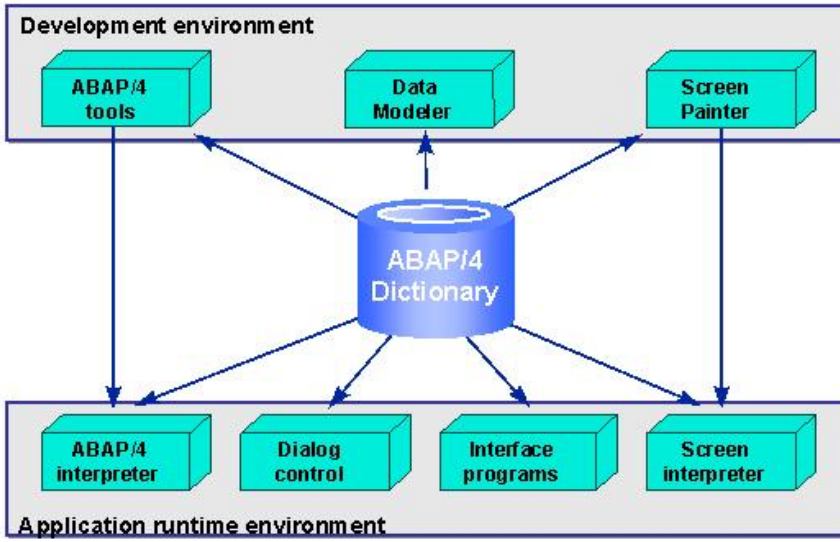
Program & Development Security

- 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.

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

Firefighter (FF) / Emergency User

- Enables users (typically support) to perform duties not in roles or profiles assigned to their user IDs (least privilege)
- Emergency, special situations:
  - Need change/update authorization in production system to fix critical problems
  - Duplicating Real world transaction use to diagnose / troubleshoot
  - Verifying Production data
  - Check production system performance.
  - Sometimes critical transactions require developer assistance to resolve issues in production environment.

- SuperUser Privilege Management (SAP GRC term)

Firefighter (FF) / Emergency User

- Each Firefighter ID:
  - Has specific authorization rights (Best practice is to distribute access among several different types of IDs – e.g. OTC, Planning, P2P)
  - Access Is pre-assigned to specific users
  - Access has a validity date.
- FF provides this extended capability to users while creating an auditing layer to monitor and record Firefighter usage
  - Reason for emergency use
  - Date / time stamps
  - What Transactions were used
  - Which updates made

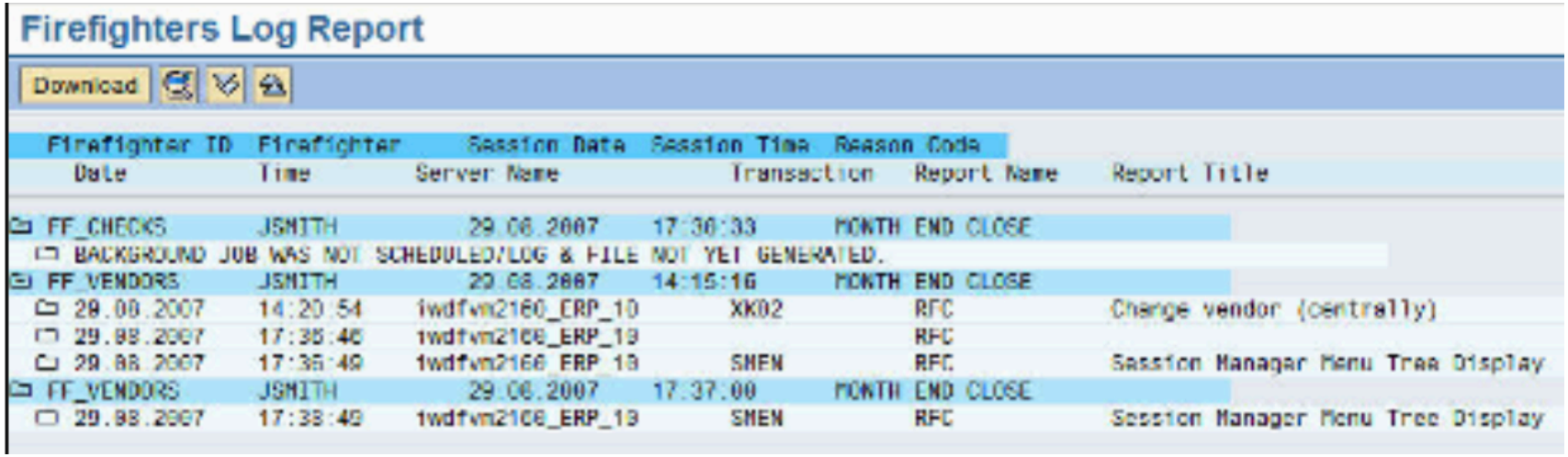
- Transaction: /n/VIRSA/VFAT

Firefighter / Emergency User

- 'Best' Practices
  - Documented FF / Emergency User Concept
  - FF focus is Production (PRD) System / clients (less to QA)
  - Do not give SAP_ALL or equivalent access to FF
  - Create FF ID for each of several useful process / support areas: e.g. (Security, IT Admin, OTC, Planning, P2P)
  - FF Used only for emergencies (not routine use)
  - Regular Support access in PRD sufficient to prevent need for routine FFID Use (good display, SPRO, low risk transactions (e.g. create Delivery))

Firefighter / Emergency User

- 'Best' Practices
  - Access only as there's a valid need – Approval needed
  - Limit access only to time needed (e.g. particular event like 'Go-Live')
  - Assure complete logging of FF Actions (config)
  - Assure audit of all access for (via reports or e-mail notification):
    - Valid Reasons -
    - Special review of all 'changes'



Risk and Recommendation
Powerful ID's and Profiles

Risks:

- SAP_ALL provides full access to the system
  - Contains * for authorizations

- SAP_NEW is an upgrade profile
  - Composite Profile contains Simple Profiles for each new release

Recommendations:

- No User should have SAP_ALL or SAP_NEW in Production (PRD) & QA
  - Basis, Security and other support personnel should not have SAP_ALL or SAP_NEW]
  - Interface and System IDs should sue custom roles (not SAP_ALL, SAP_NEW)

- Very limited (if any) Users should have SAP_ALL or SAP_NEW in Dev
  - Basis may need Dev access to SAP_ALL on occasions

Risk and Recommendation
Powerful ID's and Profiles

Risks:

- SAP* is a super user ID
  - Included with System
  - Assigned the powerful SAP_ALL profile

Recommendations:

- Change SAP* user ID password in all clients
- Lock SAP* and monitor unauthorized access attempts
- Change system parameter LOGIN/NO_AUTOMATIC_USER_SAPSTAR to 1
  - Deactivates the special default properties of SAP* (e.g. removes the ability to login to a client with a password of PASS if SAP* user master record is deleted from that client)

Note: SAP*user master record should not be deleted

GRC: Governance, Risk & Compliance

Modules (Access Control)

SAP v5.3	SAP v10.0	Function
Risk Analysis & Remediation	Access Risk Mgmt (ARM)	- SOD Rule Set (Starter rules) - Analyze and manage Access and SOD Risk (SOD, SAT Reports) - Role / User level simulation
Compliant User Provisioning	User Access Mgmt (UAM)	- Access Request & Workflow - Provision and Manage Users - Business Rules
Enterprise Role Mgmt (ERM)	Business Role Governance (BRG)	- Role Configuration - Maintain Roles (owners, mass change) - Integration with ARM prevents SOD conflicts

GRC: Governance, Risk & Compliance

Modules

SAP v5.3	SAP v10.0	Function
Superuser Privilege Mgmt	Central Emergency Access (CEA)	- Firefighter administration and access portal - Can cross SAP and other apps - Sub-process of Access Control
	Process Control	- Manage developing control process documentation - Automated control testing & monitoring - Documentation from risk / control matrix
	Risk Management	- Risk ID, scenarios - Assessment of risk (indicators) - Risk response

SAP CRM

CRM: Customer Relationship Management

Solution: managing all phases of customer interaction cycle

Security: Different paradigms vs. traditional SAP components (e.g. ECC, BI)

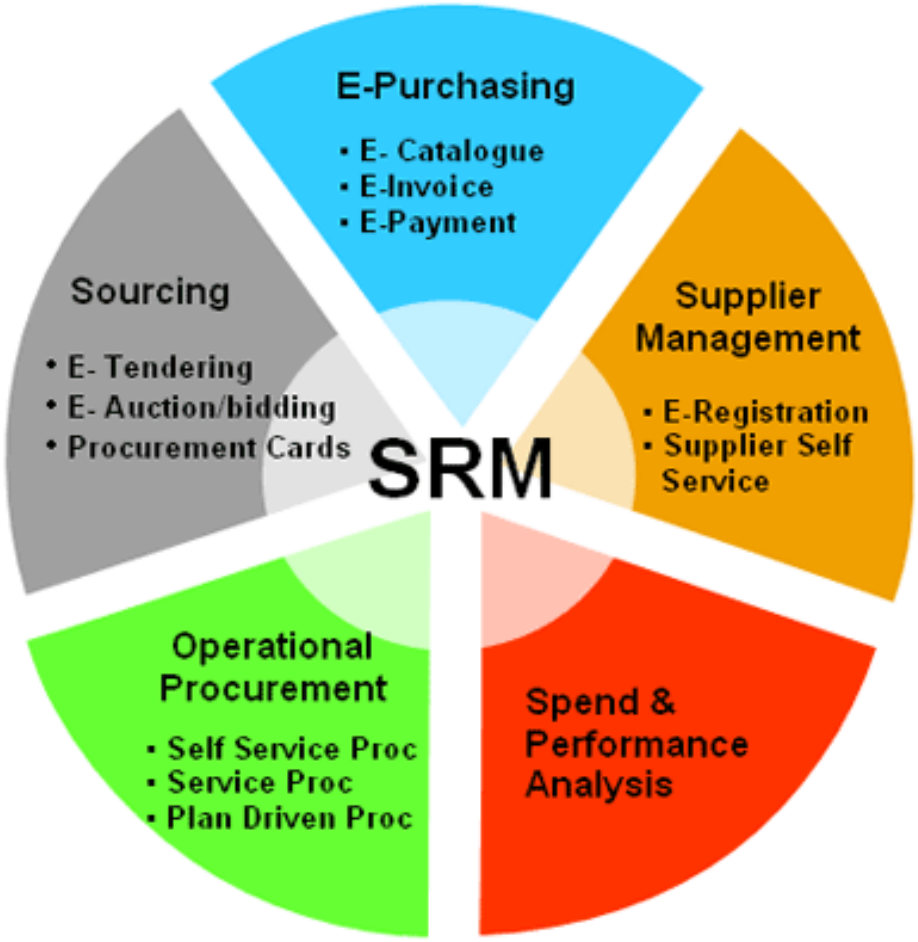
- WebClient UI links vs. traditional transactions (Internet apps)
- Role assignment by:
  - Directly via CRM User Master
  - Indirectly: User assigned a Position, Positions assigned business role
- CRM Territory Mgmt hierarchy (territory attributes further restrict access to customers and /or material)
- Use of multi-tier security restrictions

SAP SRM

SRM: Supplier Relationship Management

Solution:

- Automate / simplify Procure-to-Pay processes
- Strengthen supplier relationships



SAP SRM

SRM: Supplier Relationship Management

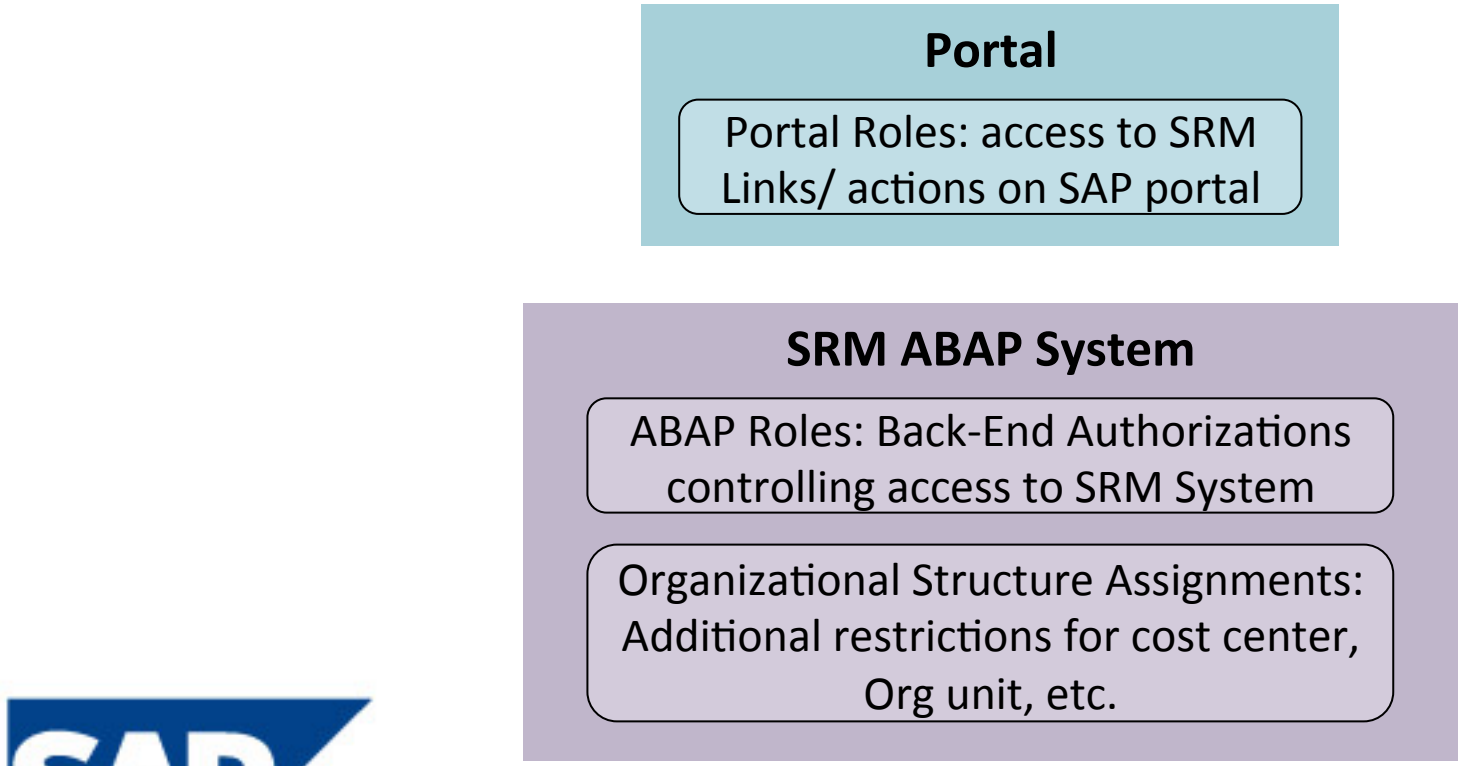
Security: Enterprise Buyer security options

- ABAP Security Roles
- SAP NetWeaver Portal Security Roles
- Organizational Structure and Attributes

Note: The 3 security layers / components must be tightly aligned and integrated to streamline the model

SAP: SRM Security Integration

Note: The 3 security layers / components must be tightly aligned and integrated to streamline the model



SAP® SRM

SAP BI

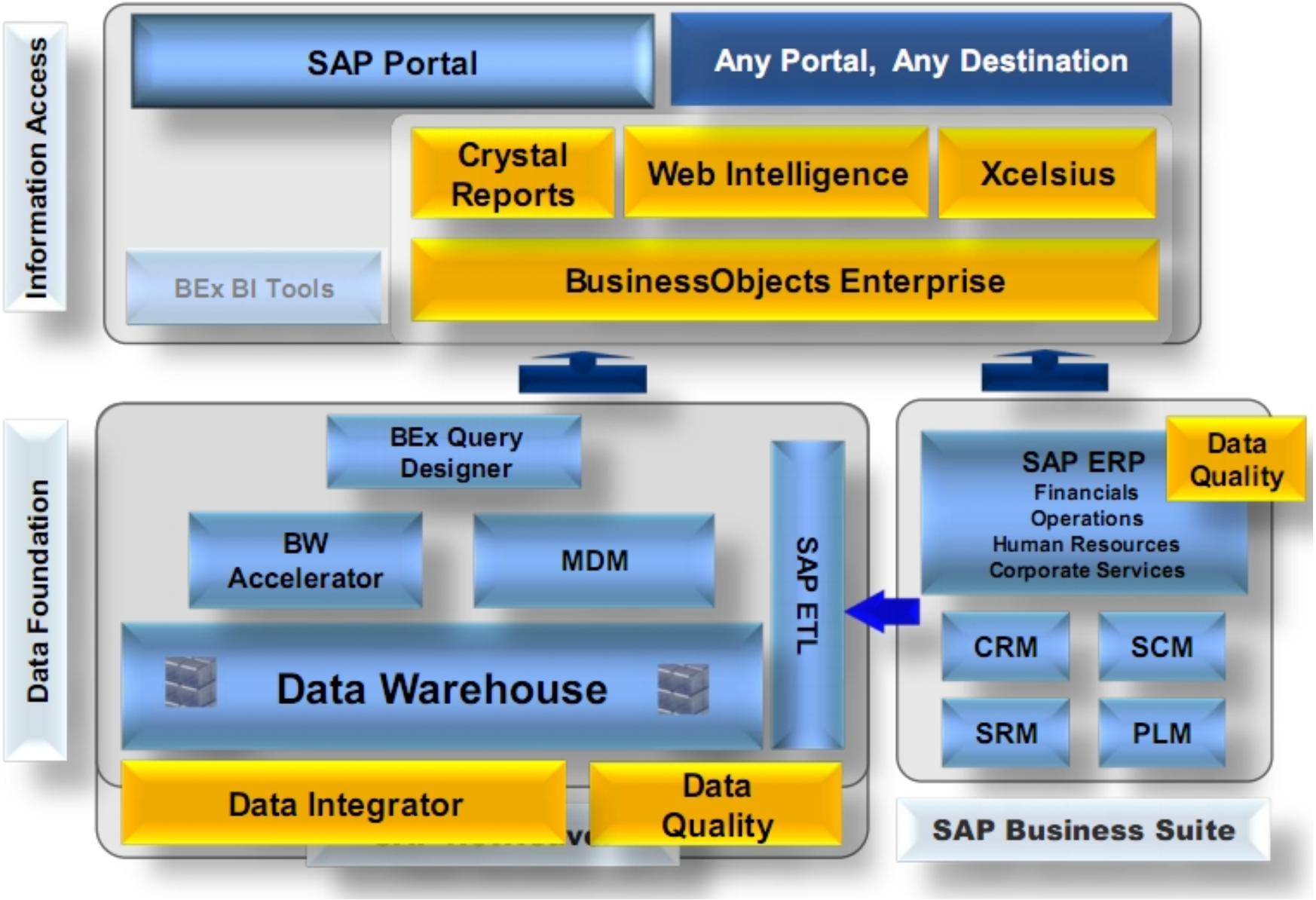
BW/BI: Business Warehouse / Business Intelligence

Solution:

- Business information for decision making
- BW – the information extractor, transform and consolidate (info-cubes) and one access tool
- BO – Business Objects: another information access tool

SAP Business Information Warehouse (SAP BW)

SAP BW Architecture



SAP BI Security

Security: is not transaction based

- Secure BW data objects:
  - Operational Data Store (typically the core data dump from process, transactions)
  - Info Cube
  - Info Source
- More detailed Security by data dimension (e.g. organizational object like company, plant, etc.)

SAP Business Information Warehouse
(SAP BW)

Segregation of Duties

Goal: prevent error and fraud

Definition

- 'ensuring that at least two individuals are responsible for the separate parts of a task'

  Person who _____ *should* ***not*** *be the person who* _____ .

- An Individual should only have 1 of following Responsibilities / Privileges:

  Authorization / **A**pproval

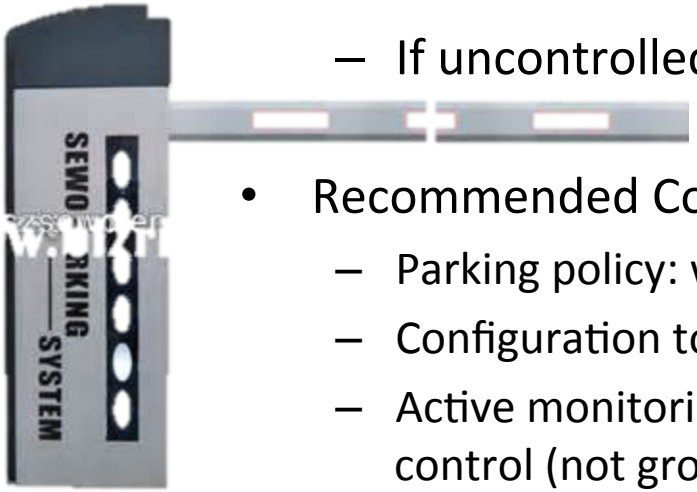
  Recording (Add, change, etc.)

  Custody of asset / resource (checks, inventory, etc.)

Finance: Document Parking

Used to enter / store (park) incomplete documents in SAP

- Risks
  - Occurrence / Existence assertions unclear (does transaction really exist?)
  - Incorrect transactions included in results
  - If uncontrolled, continued eroding validity of data / assertions



- Recommended Controls
  - Parking policy: when allowed, how resolved
  - Configuration to trigger workflow (rules based)
  - Active monitoring of parked documents (#, value, aging) to assure in control (not growing, not becoming older)
  - Audit and decision making of select entries (e.g. high value, oldest)
  - Segregation of duties
  - …

Finance: 1-time Business Partners

- Customers or vendors
  - Used for rarely used, single use business partners
  - Generic 1-time master data records created (created once)
  - Unique address, etc. for each of several real 1-time partner are maintained in transaction documents
- Risks
  - Bypasses Segregation of duties between master and transaction data processing (master data not needed)
  - No credit limit – fraudulent actions possible
  - Cash outflow to alternate payees / addresses
- Controls:
  - Don't Use
  - Analyze transaction use with 1-time partners
  - Compensating controls (e.g. authorization)

Finance: Fixed Assets

- Risks
  - Does asset exist?
  - Is it valued correctly? Capital vs. expense
  - Incorrect valuation
  - To I Own it?
  - Timing (esp. for long build projects)

- Controls:
  - Strong policies documents, trained, followed
  - Detailed audit of high value, special case assets
  - Search for Strange / different patterns of assets depreciation expense

Inventory Control: Common Risks

- Theft
- Lost Inventory / Damage
- Transaction Errors
  - Human Errors
  - System caused (e.g. BOM accuracy)
- Material Life Cycle (e.g. obsolete / scrapping) and Shelf Life
- Segregation of Duties (physical custodians vs. accounting record custodians)

Inventory Control: Common Controls

- Segregation of Duties (physical vs. record custodian)
- Inventory policies (Written, taught, monitored)
- Test inventory transactions (shipping, production, procurement, transfers, etc.)
- Inventory Record Accuracy: physical or cycle count
- Timing
- Match control / methods to size of risk (high value)

Few Remaining Topics

Types of SAP Controls

- Authorization / Application Security
- Segregation of Duties (SOD)
- Configuration
- SAP Standard
- Manual
- Monitoring

SAP Controls: Structure & Examples

Authorization / Application Security

- The ability to ***{action}*** a ***{what – include transaction codes}*** is restricted to the ***{role(s)}***

Example: The ability to create and change a purchase order via transaction codes ME21N and ME22N is restricted to purchasing buyers. This ability is restricted by company code and document type.

Segregation of Duties

- The ability to ***{action}*** a ***{what – include transaction codes}*** is restricted from***{action}*** a ***{what}***. This ability is segregated by not allowing the same functional role to perform these tasks.

Example: The ability to create and change a customer invoice via transaction codes VA01 and VA02 is restricted from the ability to create and change pricing conditions via transaction codes VK11 and VK12. In addition, this ability is limited by Sales Organization.

SAP Controls: Structure & Examples

Configuration

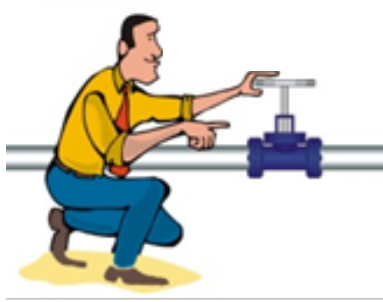
- SAP is configured ***{to do what}*** when ***{at what time / event}. {What are the limitations of the configuration}***

Example: SAP is configured with FI tolerance groups. Tolerance groups are configured based on General Ledger and Vendor Invoice with these dollar limits:

Tolerance Group ZOAP: A/P Clerks are limited to posting vendor invoices up to $250

Note: Tolerance groups are controlled by user ID and must be updated consistently to aliwith with user access (security)

SAP Controls: Structure & Examples



Manual Control

- ***{What is done}*** by ***{whom} – {when is it done}***.

Example: Company procedure xx.x.x states that vendor invoices are batched and totaled on a daily basis by Accounts Payable Clerk after approval is received (signoff) from the Accounts Payable Manager prior to being input into SAP.

Monitoring Control

- Report xxxx ***{name of report and transaction code}*** is generated ***{when is report generated}***. Report xxxx ***{provides what information}*** and includes ***{what fields of data}***. Report xxxx is reviewed by ***{whom}*** during ***{when is report reviewed}***. Discrepancies found in repot are ***{how are discrepancies documented and resolved}***.

Example: The list of GR/IR Balances via transaction code MB5S is generated monthly. The reports shows goods receipt without matches to invoice receipts. The Accounts Payable Clerk investigates and reconciles items aged greater than 60 days. Items unable to be reconciled after 120 days are investigated by the Accounts Payable Clerk and Accounts Payable Manager until the goods receipt or invoice receipt is cleared.

SAP Standard Controls

- SAP automatically ***{does what}*** – ***{when is it done}***.

Examples:

- Journal entries must balance (debits = credits)
- Automatic integration and posting
- All transactions generate unique documents
- History of transactions executed by users
- Logging and history of program change
- Document principle
- Online data analysis

Document Principle

- A document is a discrete object in SAP that stores data related to a single business transaction
- All SAP transactions are stored as documents
- All documents are assigned a unique identifying number
- The documents remains a coherent unit
- Only complete documents can be posted
- Incomplete documents can be stored by holding or parking
- A document consists of header and line items
- Sample and recurring documents may be used to simplify data entry tasks

Document Examples

- Purchase Order
- _____
- _____
- _____
- _____
- _____
- _____
- _____

Document Examples

- Sales Order
- Purchase Order
- Delivery
- Customer Invoice
- General Ledger Posting
- Vendor Invoice
- Material Movement

Question & Answers

- Your chance to ask me questions related to course topic - I'll attempt to answer or get you an answer

- *Each person must ask minimum of 1 question*

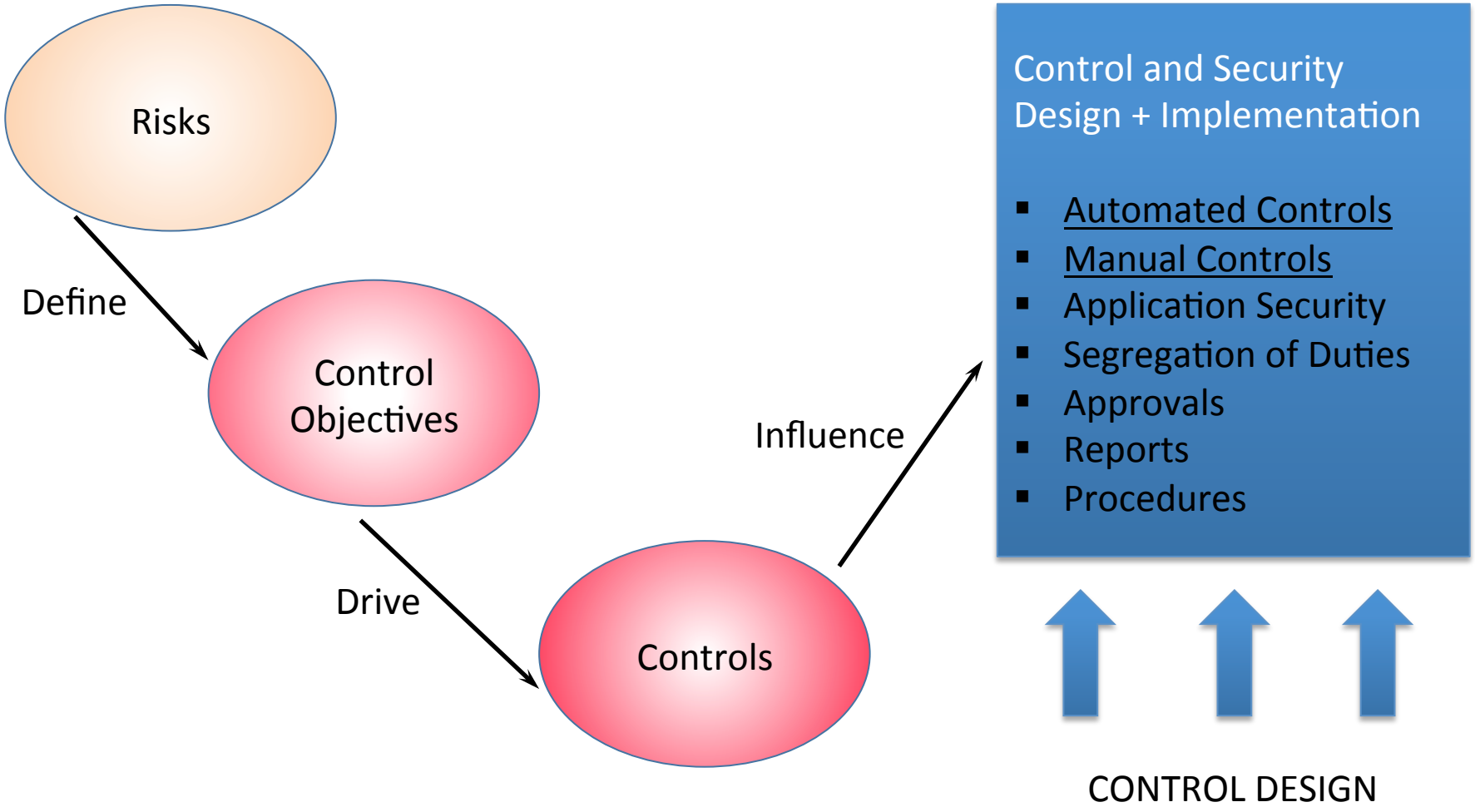
Break Time

Risk / Control Matrix
Final Exercise

Risk / Control Matrix: Final Exercise

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

Risk / Control Matrix: Design Approach



Risk / Control Matrix: Final Exercise

Part 4: Augment key controls information for the Order to Cash (OTC) process at GBI

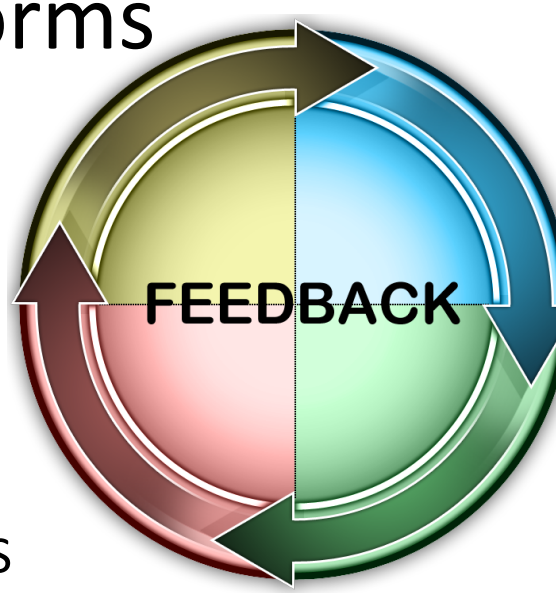
- Tab: Part 2 – GBI Controls
- Control Description (Columns F -> I) Mark each using taxonomy provided
  - Control Owner (Title): Choose **one** title from Appendix 1 or define appropriate missing title
- Financial Statement Assertions (Columns J -> O) Mark with **X**
- Risk Assessment of control (Columns P -> S)
- Financial Statement Impact (Columns T -> AI) Mark statements impacted with **x**

Risk / Control Matrix: Final Exercise

Part 5: Create Control Process and Auditing Documentation for the Order to Cash (OTC) process

- Appendix 2 and 3 of the Exercise Guide has documentation examples from the Procure to Pay process:
  - Appendix 2: Automated Configuration Control
  - Appendix 3: Manual Monitoring Control
- Using these examples and format, create **one** example document for one of your identified OTC Controls (Part 3)
- Submit as separate Word document or insert as tab in Submission Spreadsheet
- Resources:
  - Professor: in class, e-mail, phone (609-206-9783)
  - Table TSTC (List of transaction codes – reports)

SFF: Student Feedback Forms



- Value
  - ❖ Your feedback already (after tests, etc.) has already helped me improve the class
  - ❖ You wouldn't have Exam Guides for Exam 3 without your feedback
  - ❖ Better class for subsequent students and to FOX MIS in total

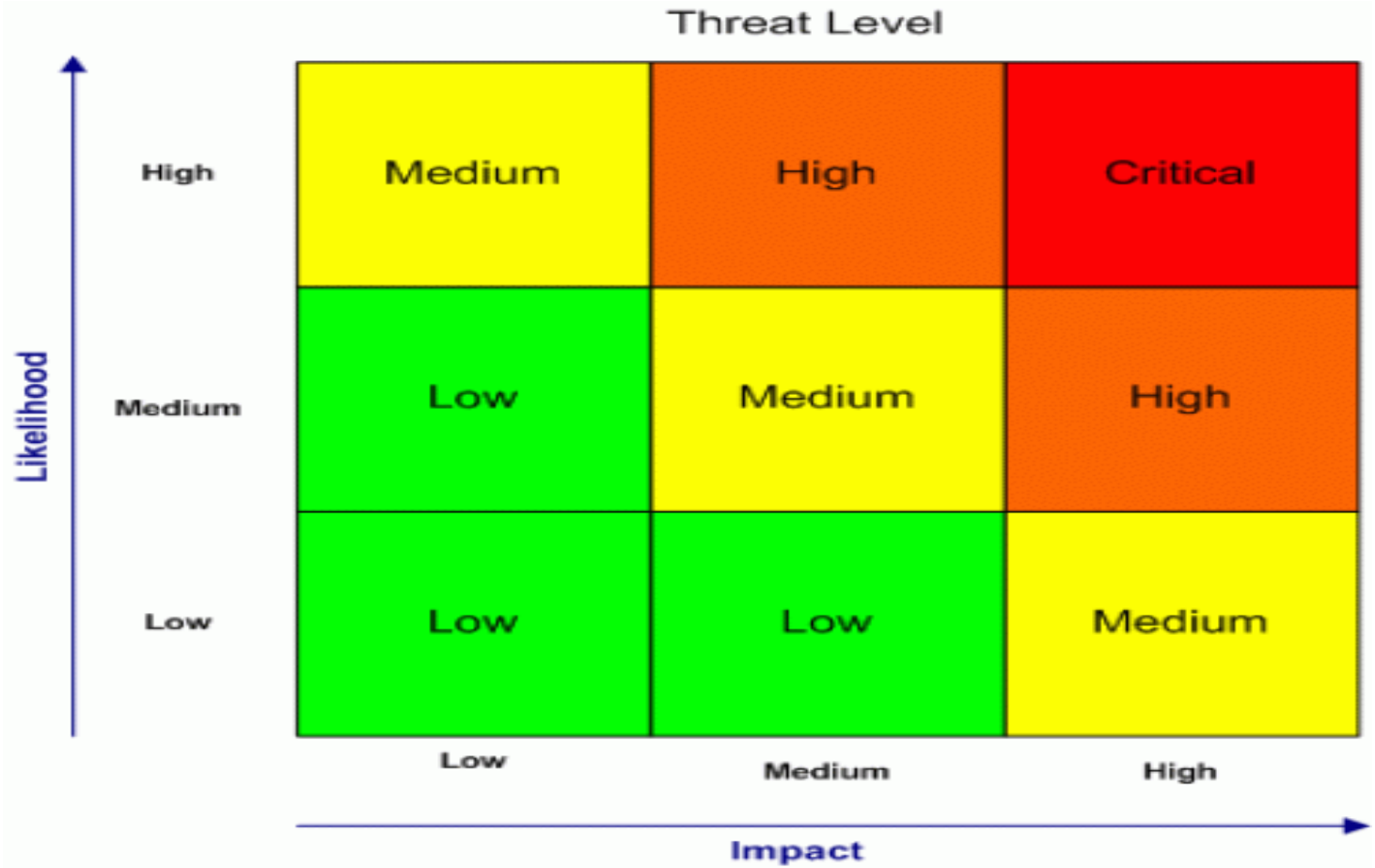
- Request
  - ❖ Have received the e-SFF e-mail??
  - ❖ Take 10-15 minutes to complete: next class
  - ❖ http://esff.temple.edu

-

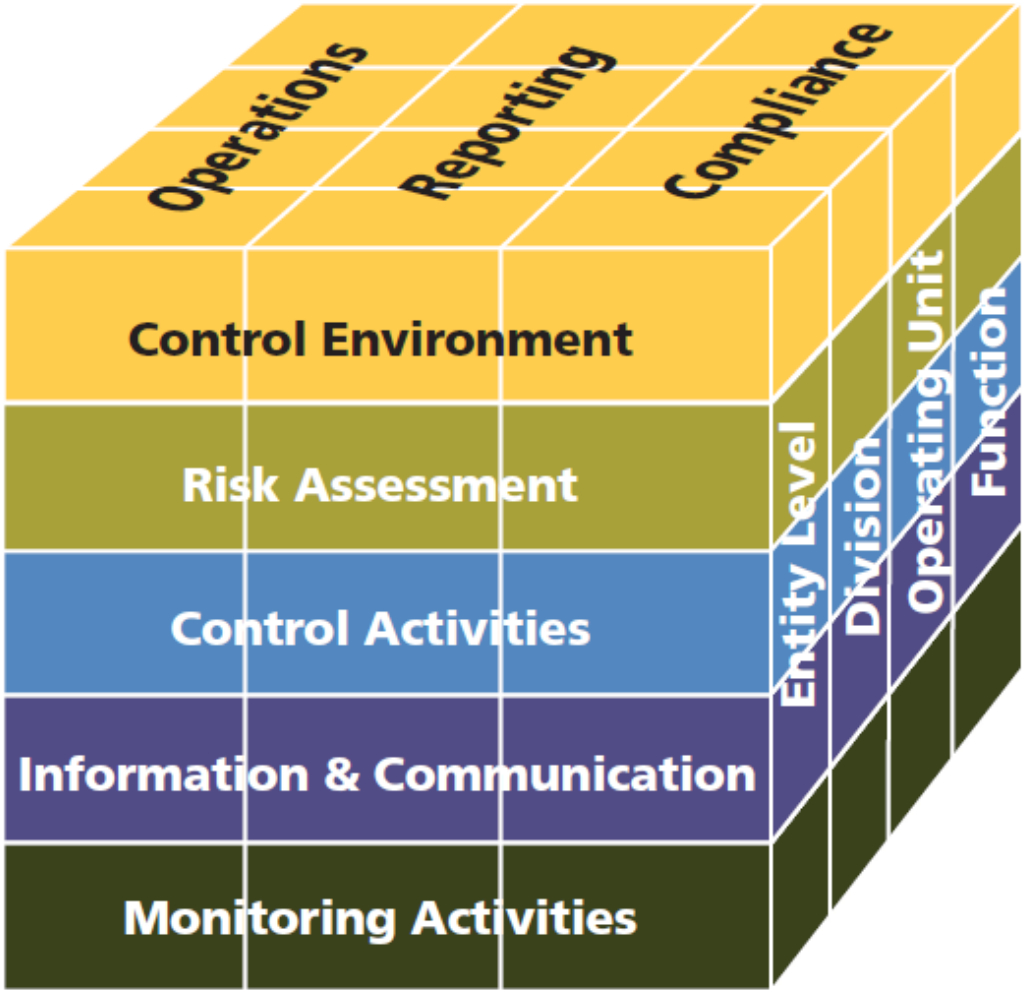
Extra Slides

Risk Assessment

Extra Slides



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

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

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)