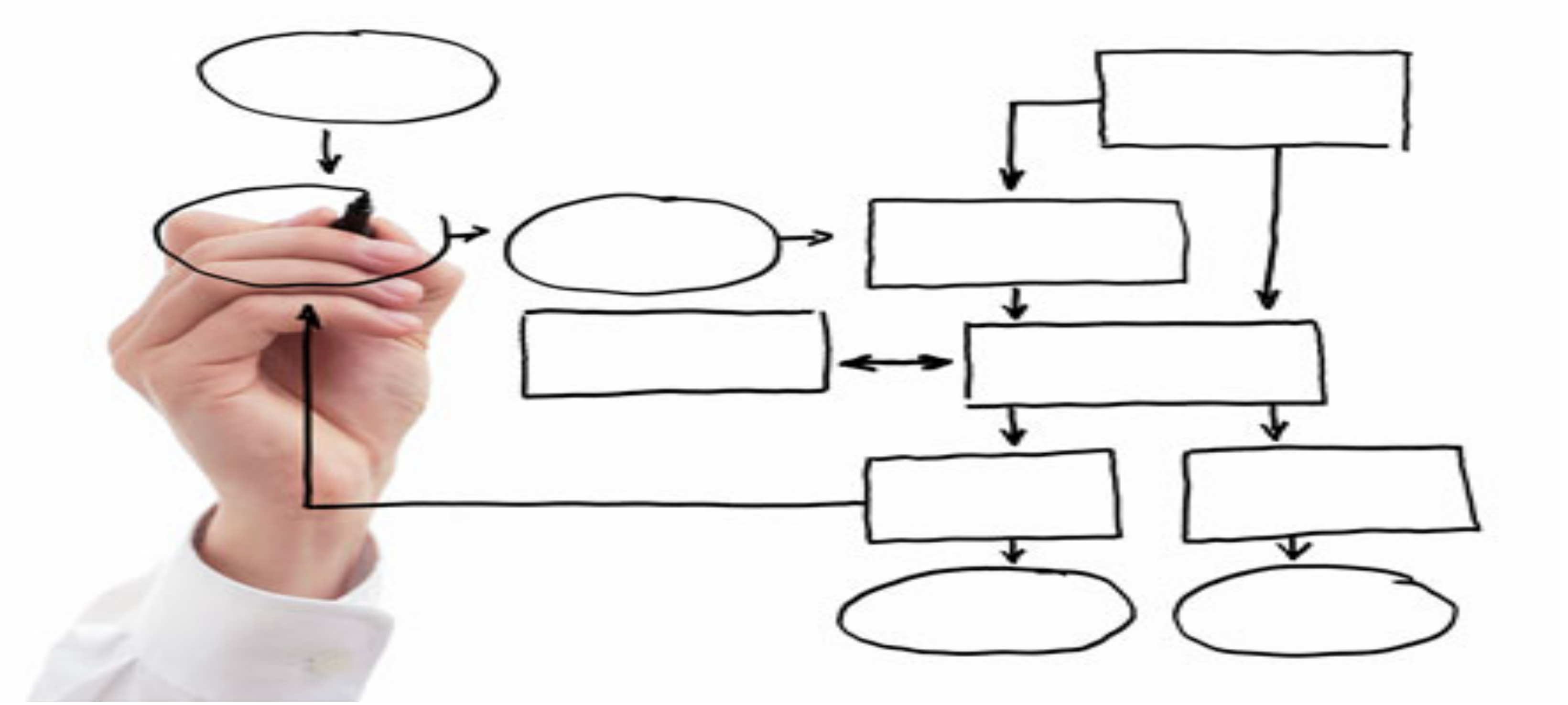


MIS 5121:Business Processes, ERP Systems & Controls
Week 11: *Change Management, IT Controls Framework*

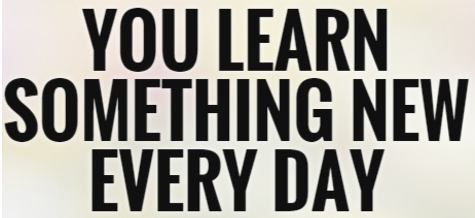
FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu
ff

Video: Record the Class

Discussion

- ❖ Something really new, different you learned in this course in last week

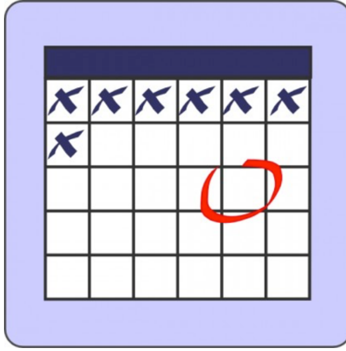


YOU LEARN SOMETHING NEW EVERY DAY

- ❖ Questions you have about this week's content (readings, videos, links, …)?

- ❖ Question still in your mind, something not adequately answered in prior readings or classes?

MIS 5121: Upcoming Events



- Guest Moderator: Auditor’s Perspective - *Week 12??*

- Guest Moderator: SAP Futures - Week 13??

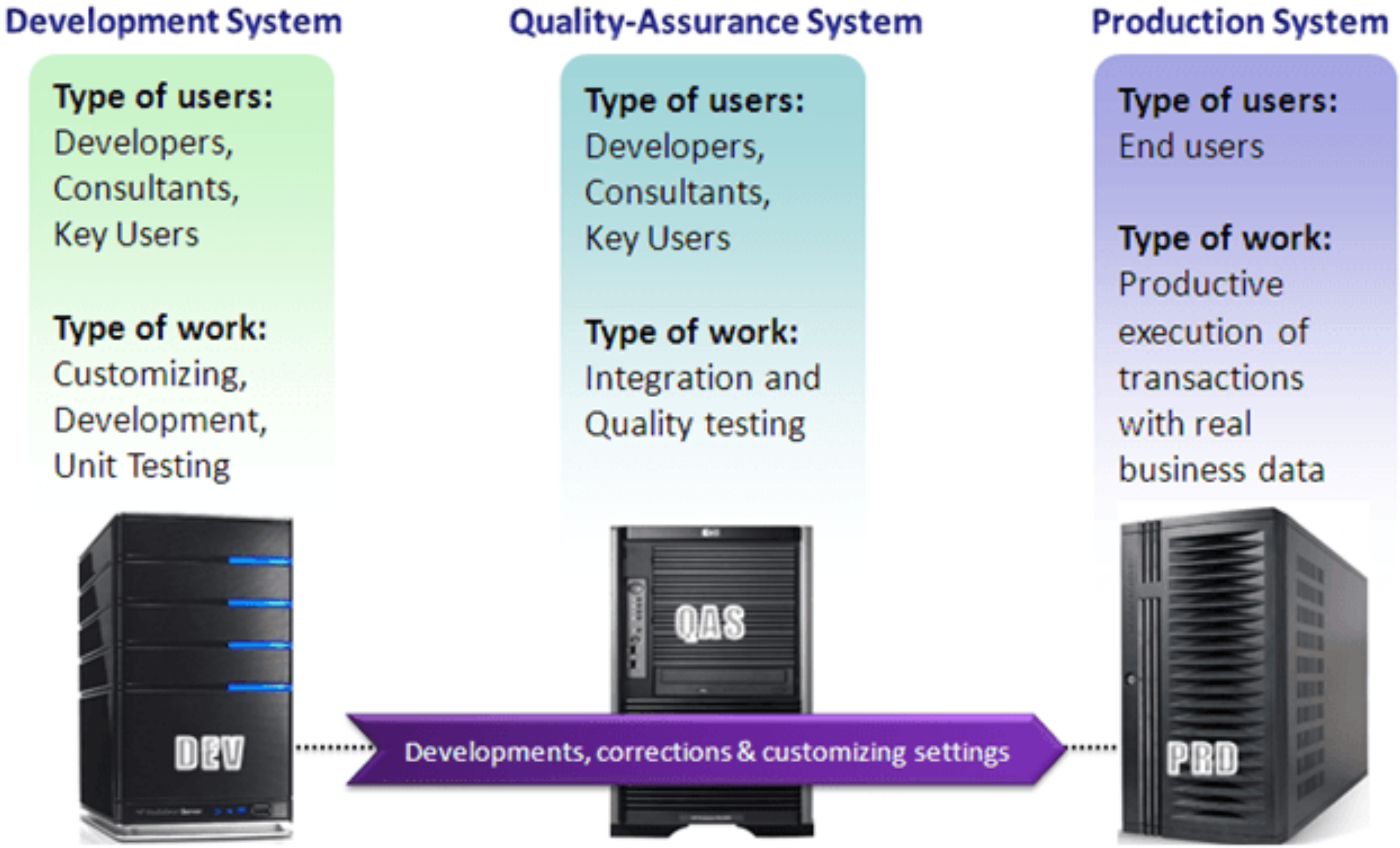
- Final Exercise (Risk Control Matrix)-*Due: December 15*

Change Management
SAP: Transport Management

Key Information Technology Risks

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

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

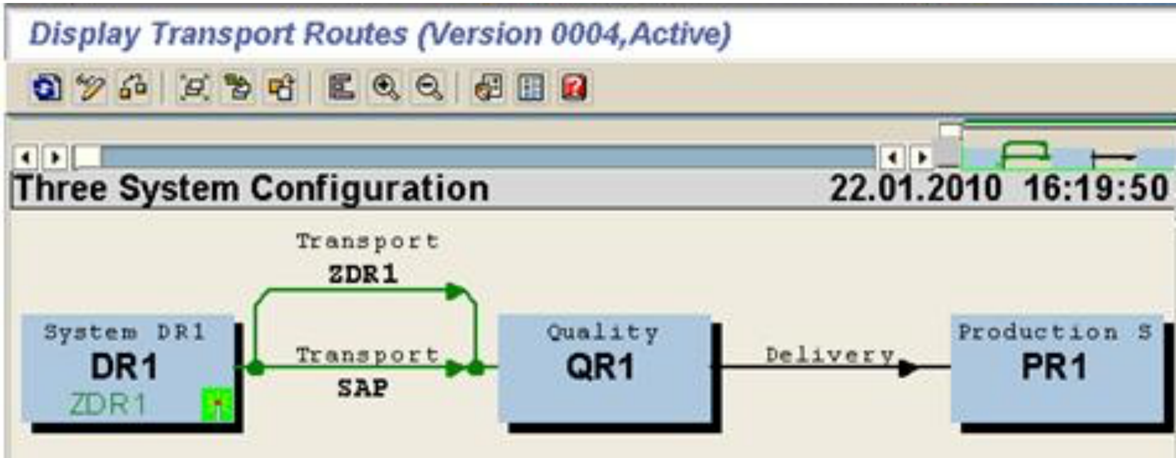
Type of users: End users

Type of work: Productive execution of transactions with real business data

Developments, corrections & customizing settings

SAP Change Management

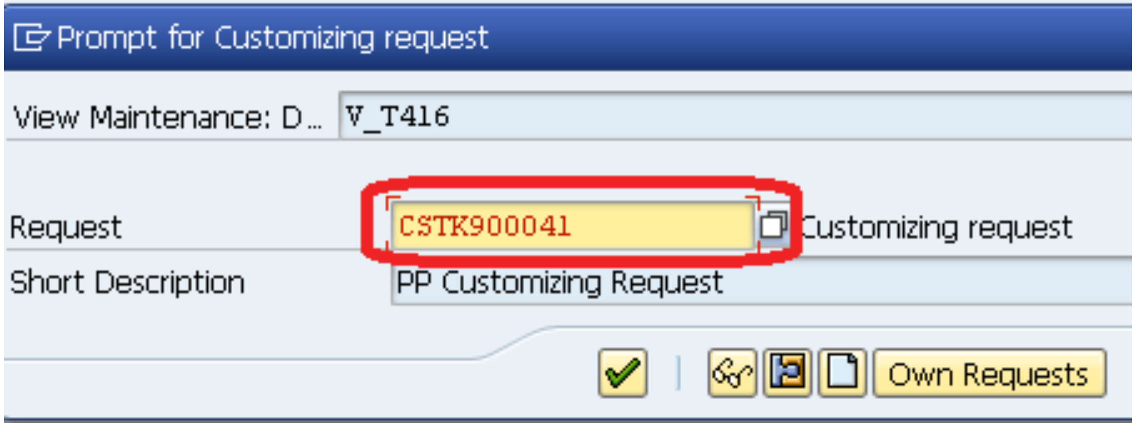
- SAP’s Correction and Transport System (CTS) provides framework for proper change control process
- SAP’s TMS (Transport Management System) is subset of CTS
- TMS Transport Routes / Paths (transaction STMS) move changes between Clients / Instances (e.g. to test, Production)
- Transaction STMS


Display Transport Routes (Version 0004,Active)

Three System Configuration 22.01.2010 16:19:50

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



Prompt for Customizing request

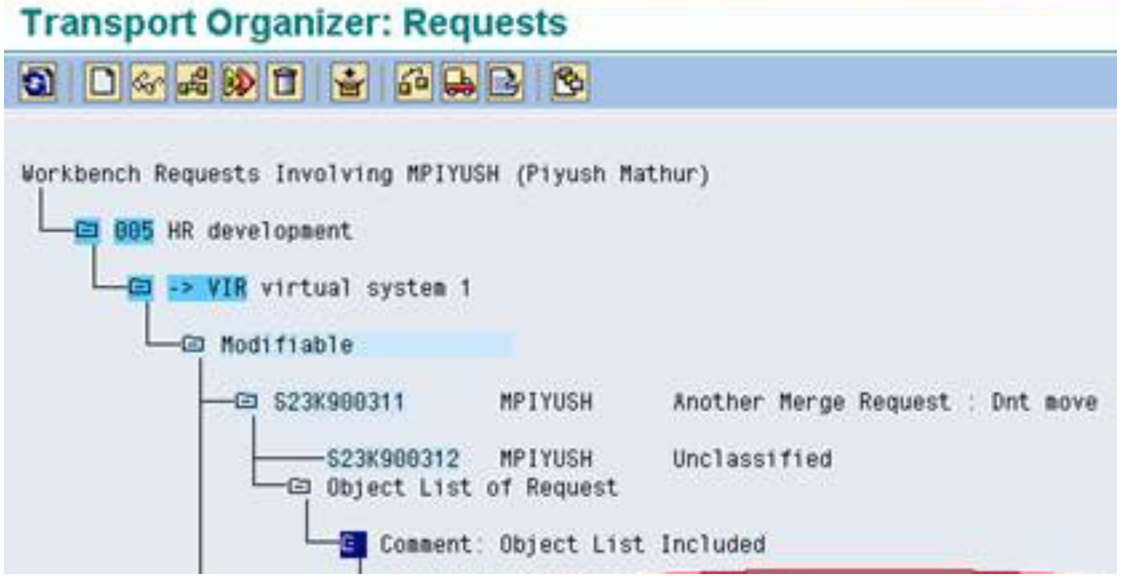
View Maintenance: D... V_T416

Request CSTK900041 Customizing request

Short Description PP Customizing Request

TMS Terminology

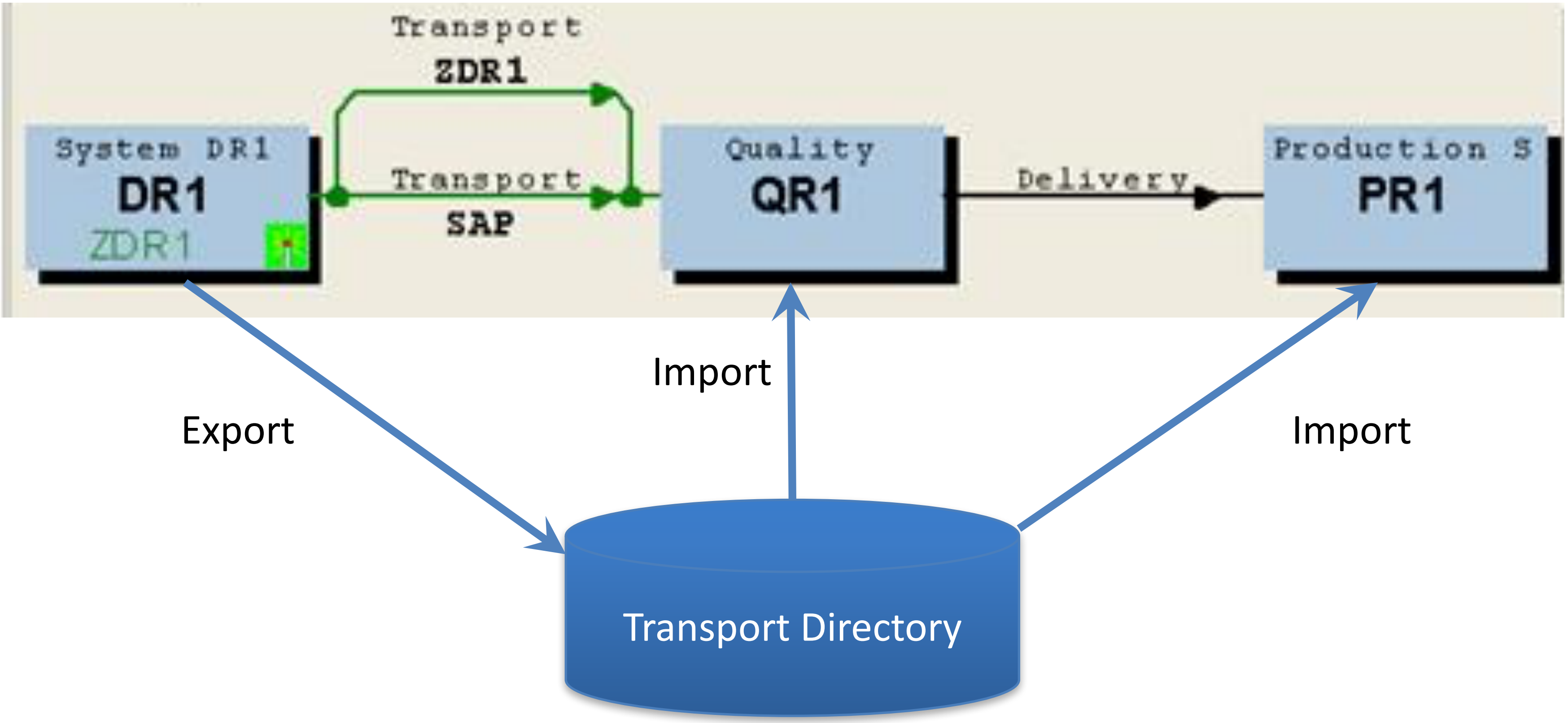
- Transport (the truck icon): contains the changes (including role changes) moved from client to client and system to system per transport path
- User ‘owns’ the change request and it’s details.
- User must ‘release’ transport prior to migration



Transport Organizer: Requests

```
Workbench Requests Involving MPIYUSH (Piyush Mathur)
 └─ 005 HR development
     └─ -> VIR virtual system 1
         └─ Modifiable
             ├─ S23K900311        MPIYUSH     Another Merge Request : Dnt move
             │   ├─ S23K900312    MPIYUSH     Unclassified
             │   └─ Object List of Request
             │       └─ Comment: Object List Included
```

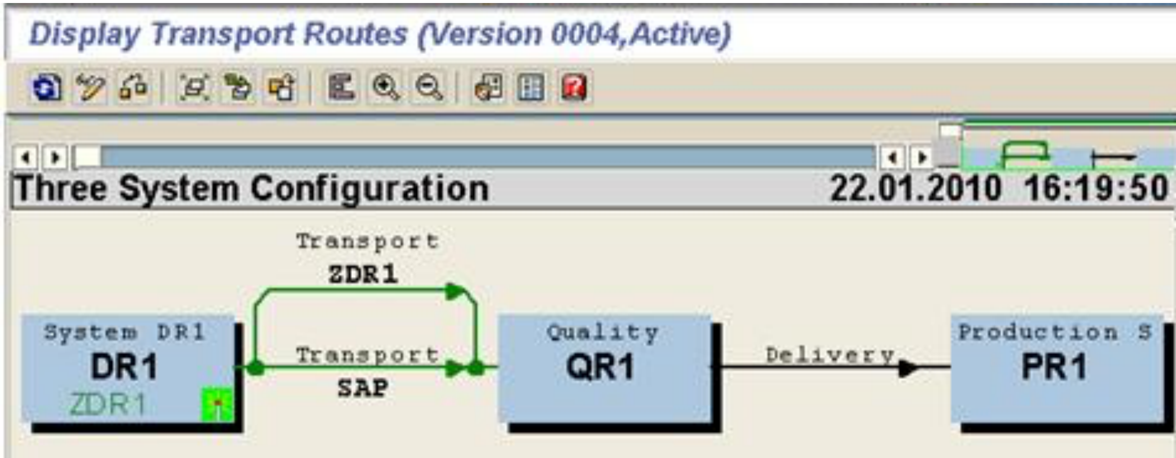
Transport Process



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

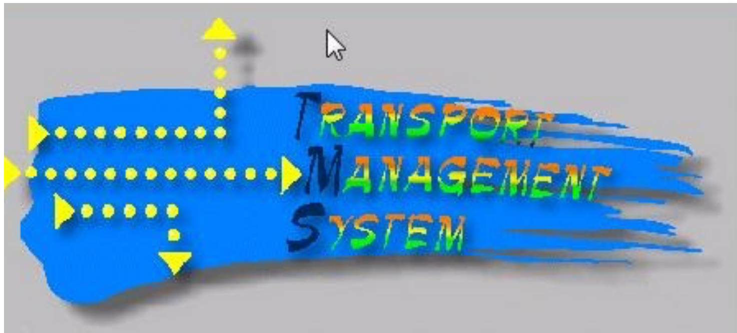


Display Transport Routes (Version 0004,Active)

Three System Configuration 22.01.2010 16:19:50

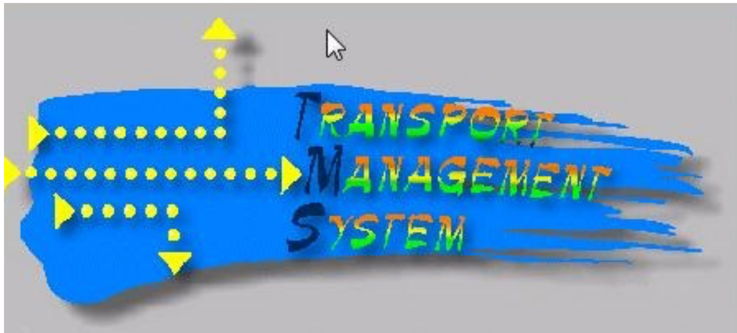
Transport Process

- 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

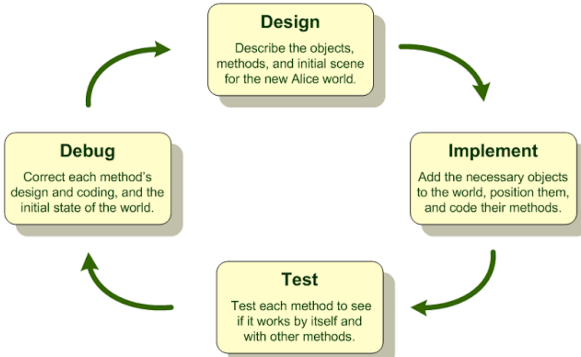


Transport Controls

- 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

Program & Development Security

- Types of Development Objects (FRICE)
  - **F**orms – outputs (invoices, Purchase orders, ...)
  - **R**eports – custom reports
  - **I**nterfaces – SAP to other systems
  - **C**onversions – Data migration
  - **E**nhancements – 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)



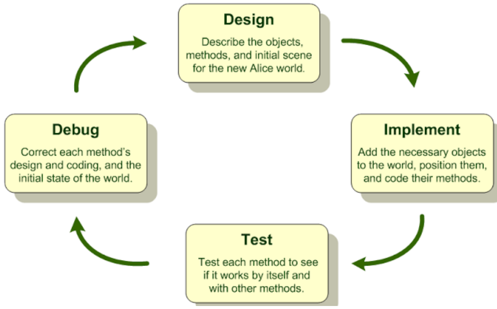
Design
Describe the objects, methods, and initial scene for the new Alice world.

Implement
Add the necessary objects to the world, position them, and code their methods.

Test
Test each method to see if it works by itself and with other methods.

Debug
Correct each method's design and coding, and the initial state of the world.

Program & Development



Design

Describe the objects, methods, and initial scene for the new Alice world.

Implement

Add the necessary objects to the world, position them, and code their methods.

Test

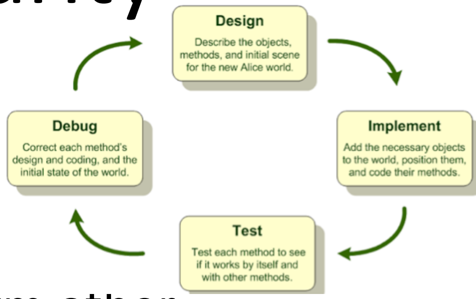
Test each method to see if it works by itself and with other methods.

Debug

Correct each method's design and coding, and the initial state of the world.

- 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



Design
Describe the objects, methods, and initial scene for the new Alice world.

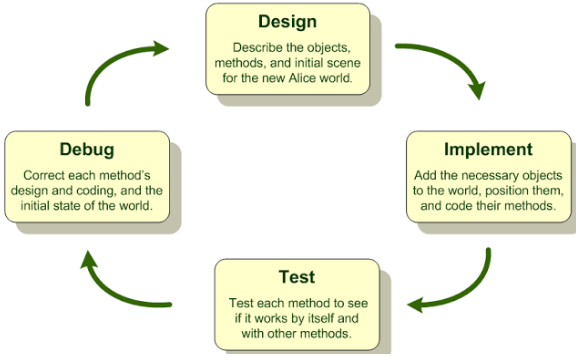
Implement
Add the necessary objects to the world, position them, and code their methods.

Test
Test each method to see if it works by itself and with other methods.

Debug
Correct each method's design and coding, and the initial state of the world.

- 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



Design

Describe the objects, methods, and initial scene for the new Alice world.

Implement

Add the necessary objects to the world, position them, and code their methods.

Test

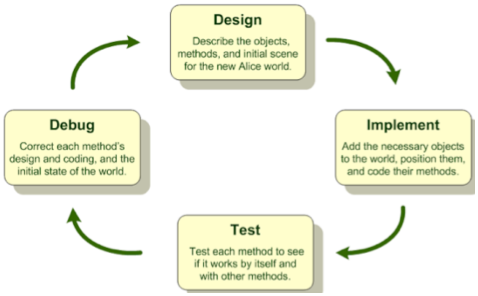
Test each method to see if it works by itself and with other methods.

Debug

Correct each method's design and coding, and the initial state of the world.

- 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



Design

Describe the objects, methods, and initial scene for the new Alice world.

Implement

Add the necessary objects to the world, position them, and code their methods.

Test

Test each method to see if it works by itself and with other methods.

Debug

Correct each method's design and coding, and the initial state of the world.

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:

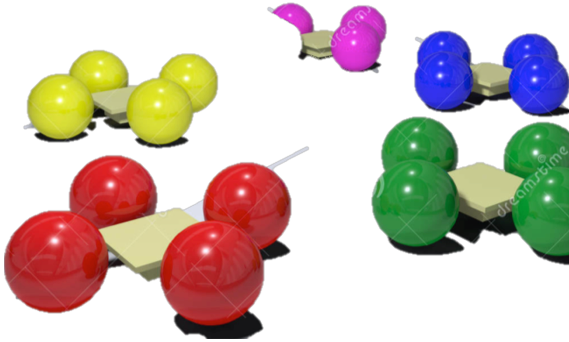
- Active review, manage program code deails
- Access to run programs restricted via SAP Security / Authorizations
- Further secure programs via assignment to authorization groups
- Basis Admin no Display access to ABAP code (prevent backdoor access)
- Debug authority restricted to effectively monitored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

Change Management /
Transport Management Overview

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

- Program Development
  - What is Development
  - Good Development Practices (Few)
  - Risks (few) and Recommendations (Few)

Breakout Activity – Rules



- Break into teams – max of 5 people / team
  - Diversity a must.
- Assignment – return via WebEx Notes or Word Document
- How: WebEx breakout?
- Time: assigned today 20 min (including break)
  - Start back **on-time**

Breakout Question

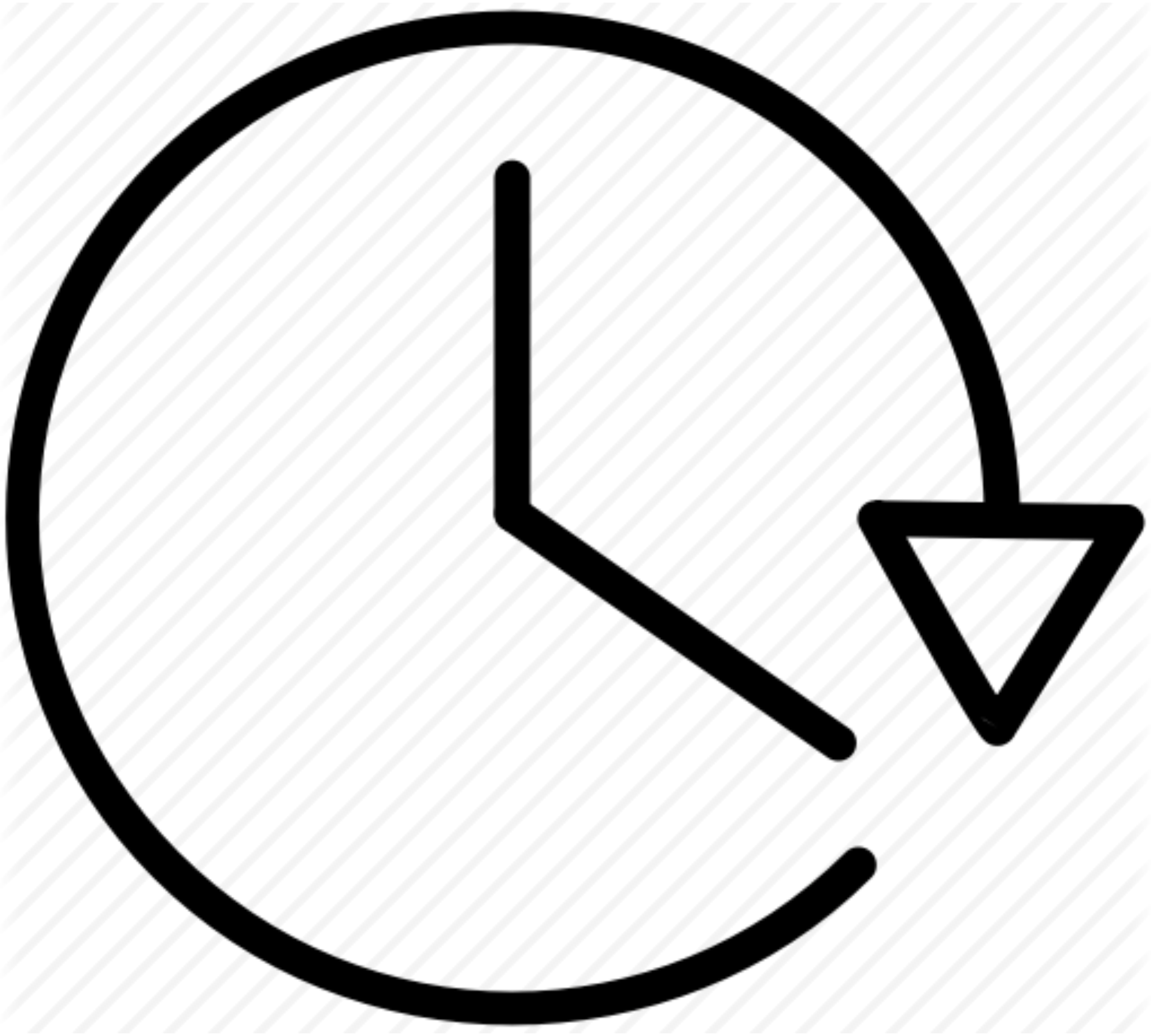
Change Management - Answer one of these Questions

Change Management practices may seem bureaucratic and time consuming. How do you manage the trade-off of added work vs. needed controls?

- ______________
- ______________
- ______________

What are the ramifications of managing change management in the scenario where the changes (e.g. development, etc.) are outsourced?

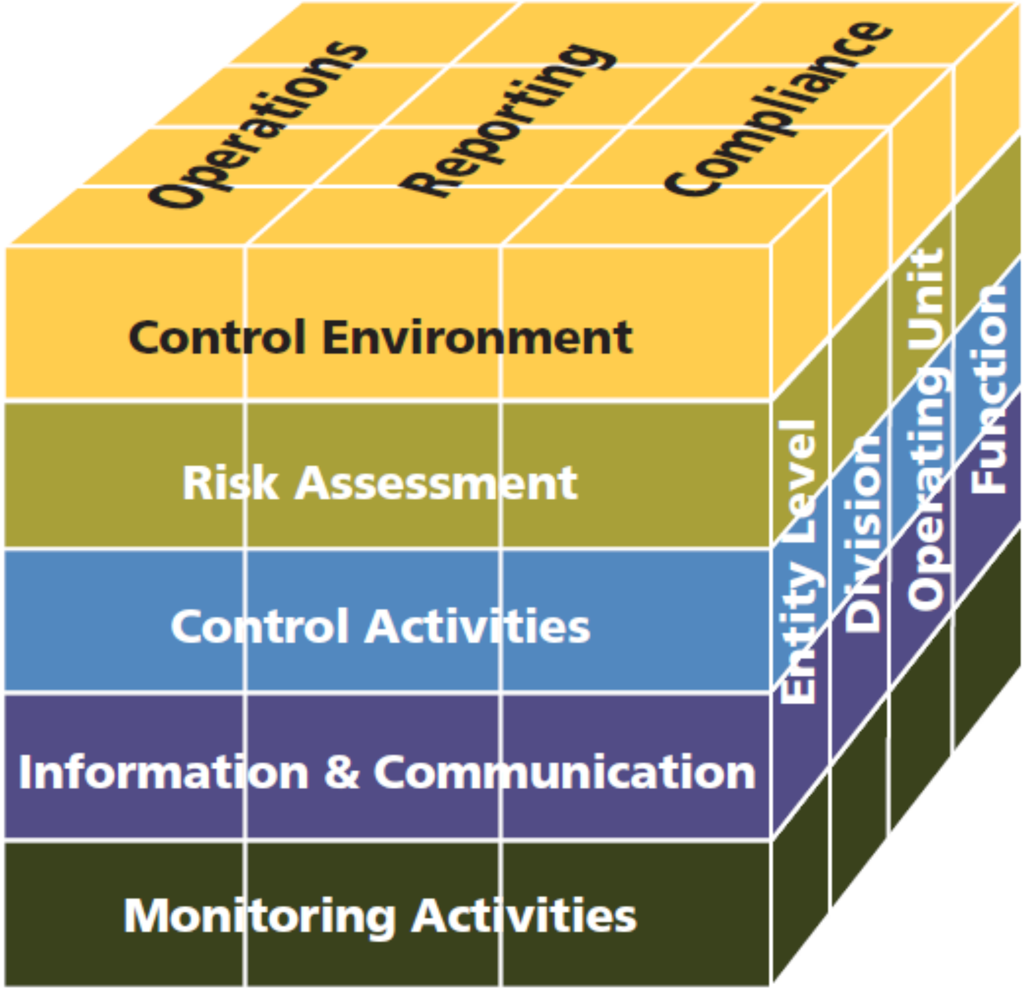
- _________________
- _________________
- _________________



Report Back

Risk / Control Matrix
Final Exercise

COSO Framework (2013)

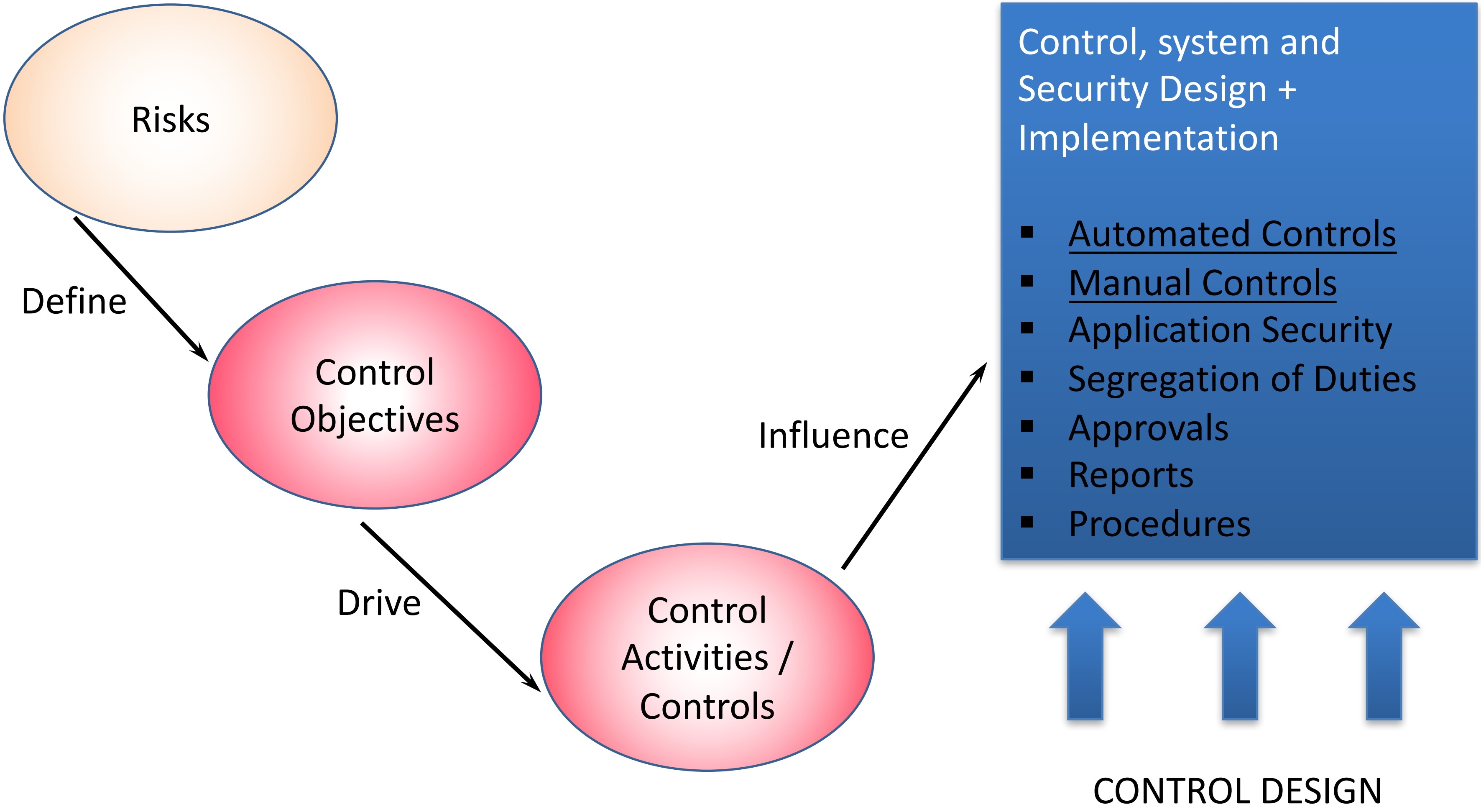


COSO Framework (2013)

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: Design Approach



Control, system and Security Design + Implementation

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

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.

Risk / Control Matrix: Final Exercise

- Agenda
  - **This Class *(November 14)*: Part 1 (Identify Risks)**
  - Future Class *(November 28)*: Part 2, 3 (Identify Controls, Link Controls to Risks)
  - Future Class *(December 5)*: Part 4 (Complete Control Definitions)
  - Future Class *(December 12)*: Part 5, 6 (Control Process / Audit Details; Personal Questions)
  - *Due December 15 11:59 PM:* Assignment Submission

Risk / Control Matrix: Final Exercise

Part 1:

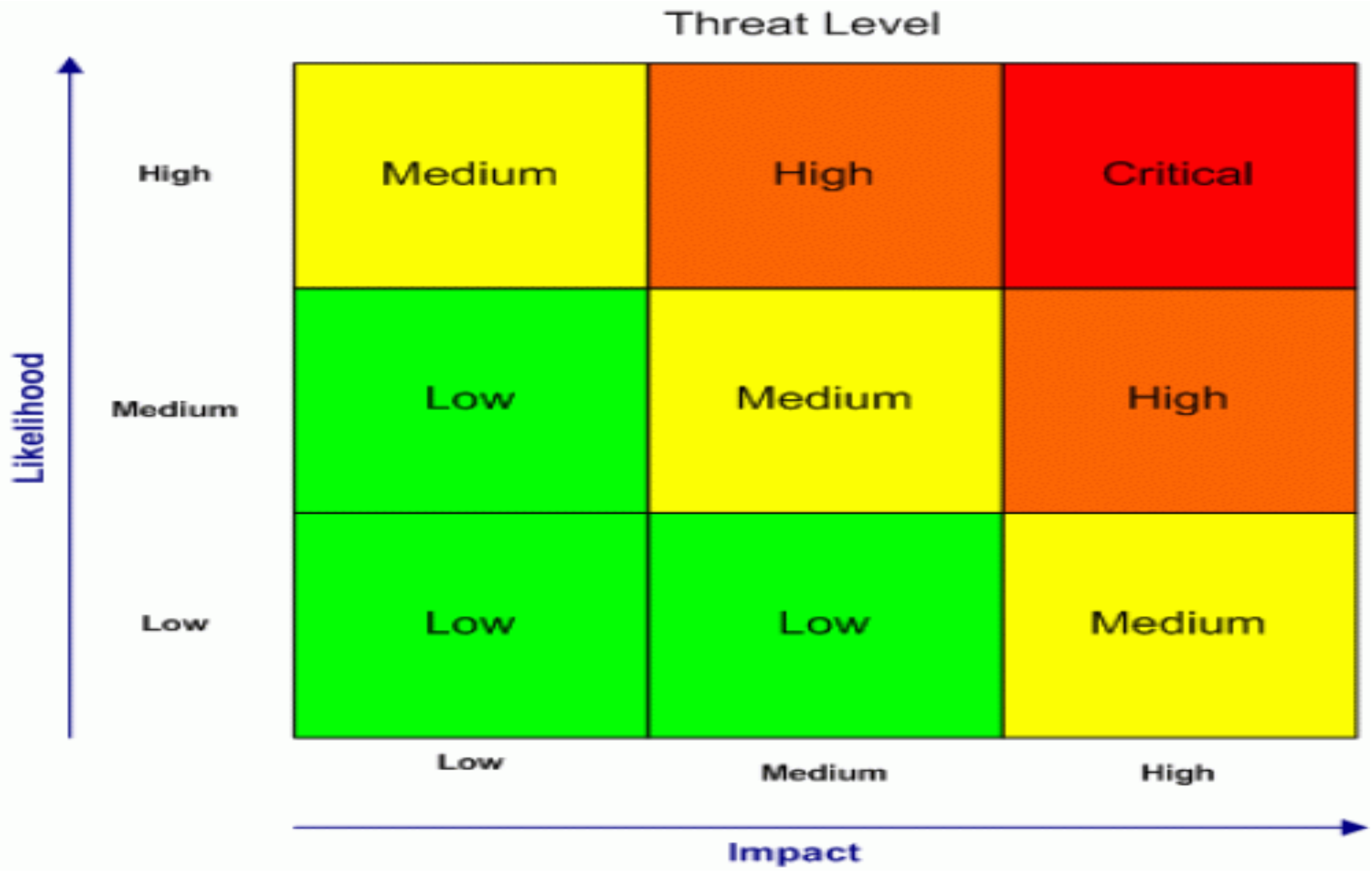
a) Analyze the key risks that exist for the Order to Cash (OTC) process at GBI

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

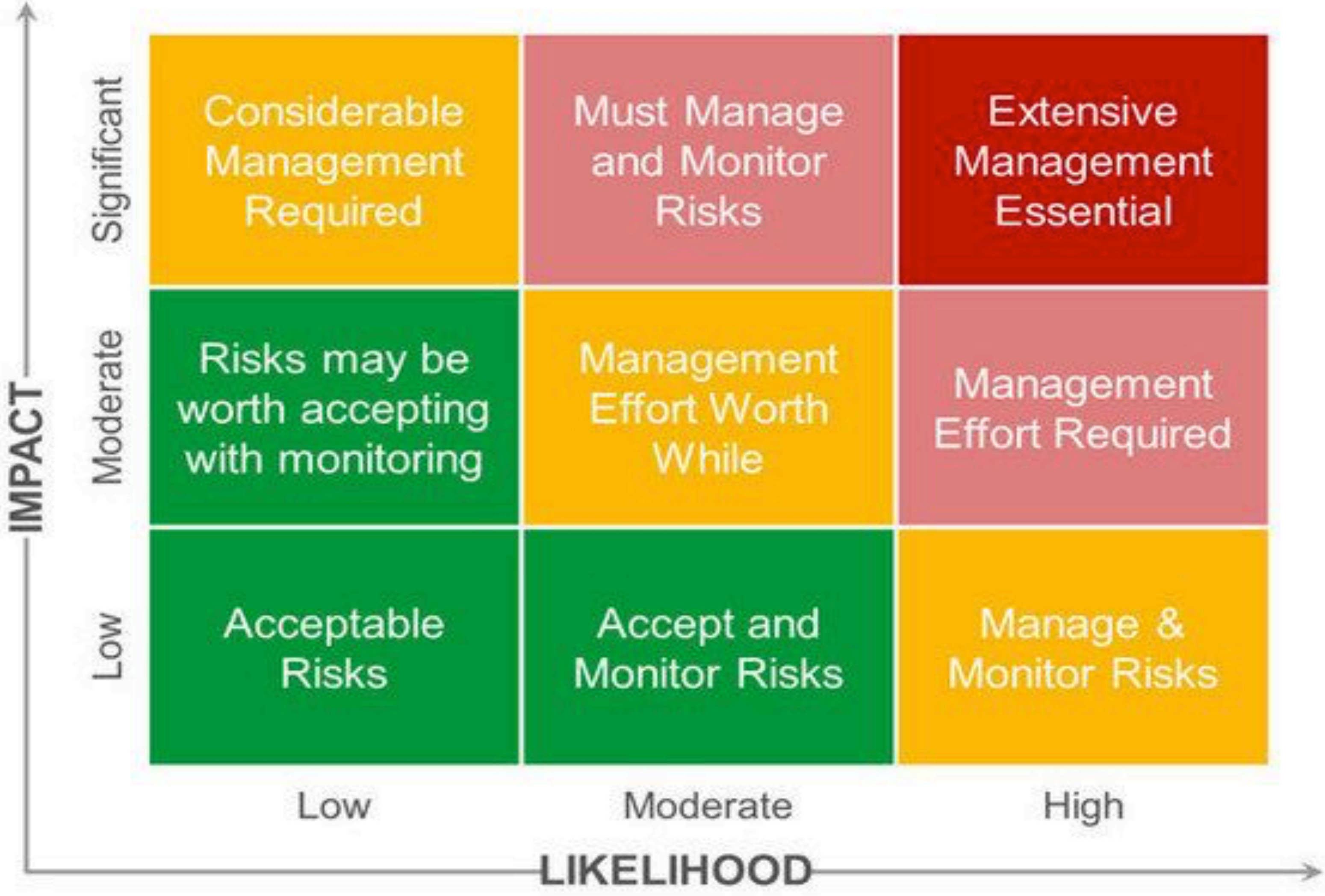


Threat Level

Likelihood	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Impact

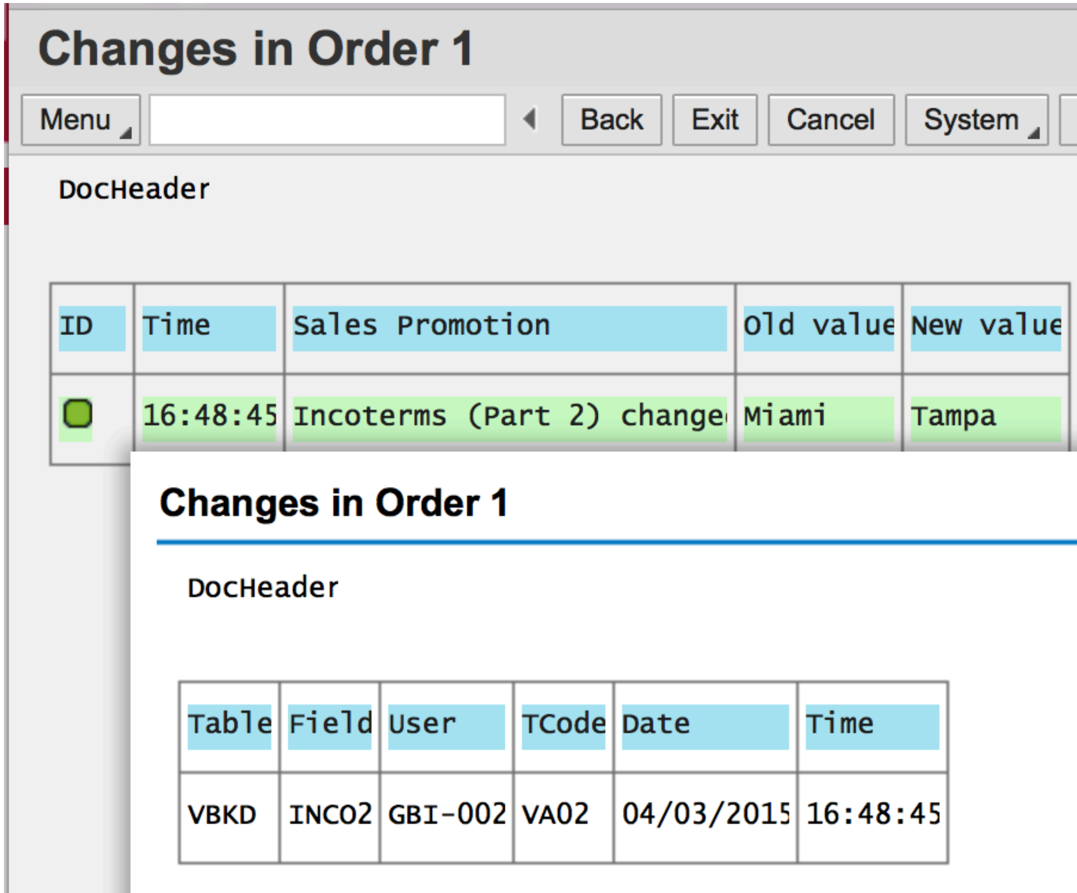
Risk Assessment



IMPACT			
Significant	Considerable Management Required	Must Manage and Monitor Risks	Extensive Management Essential
Moderate	Risks may be worth accepting with monitoring	Management Effort Worth While	Management Effort Required
Low	Acceptable Risks	Accept and Monitor Risks	Manage & Monitor Risks
	Low	Moderate	High
		LIKELIHOOD	

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



Changes in Order 1

DocHeader

ID	Time	Sales Promotion	Old value	New value
🟩	16:48:45	Incoterms (Part 2) change	Miami	Tampa

Changes in Order 1

DocHeader

Table	Field	User	TCode	Date	Time
VBKD	INCO2	GBI-002	VA02	04/03/2015	16:48:45

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

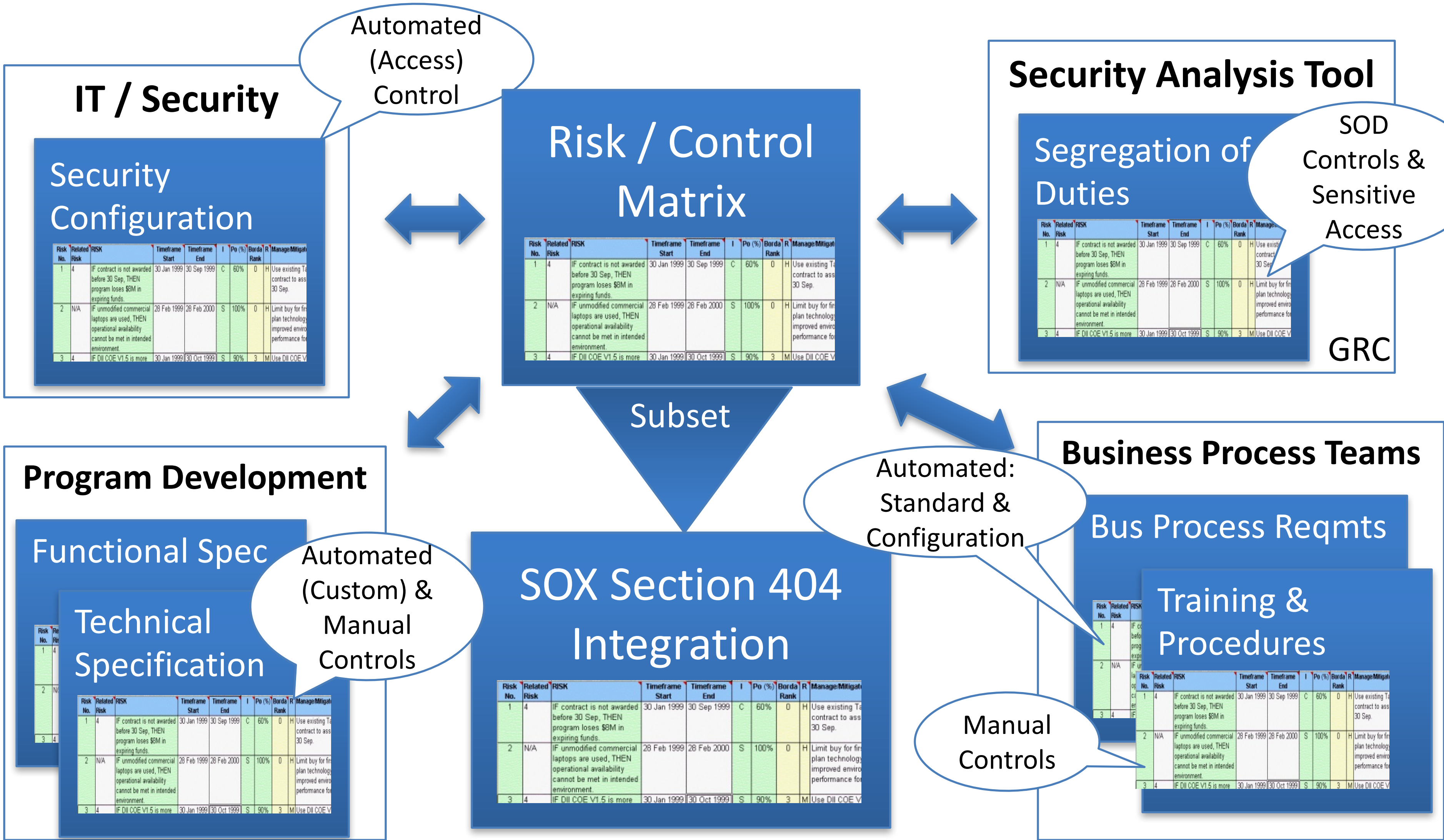
Recommendations:

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)

Controls: Integration Points

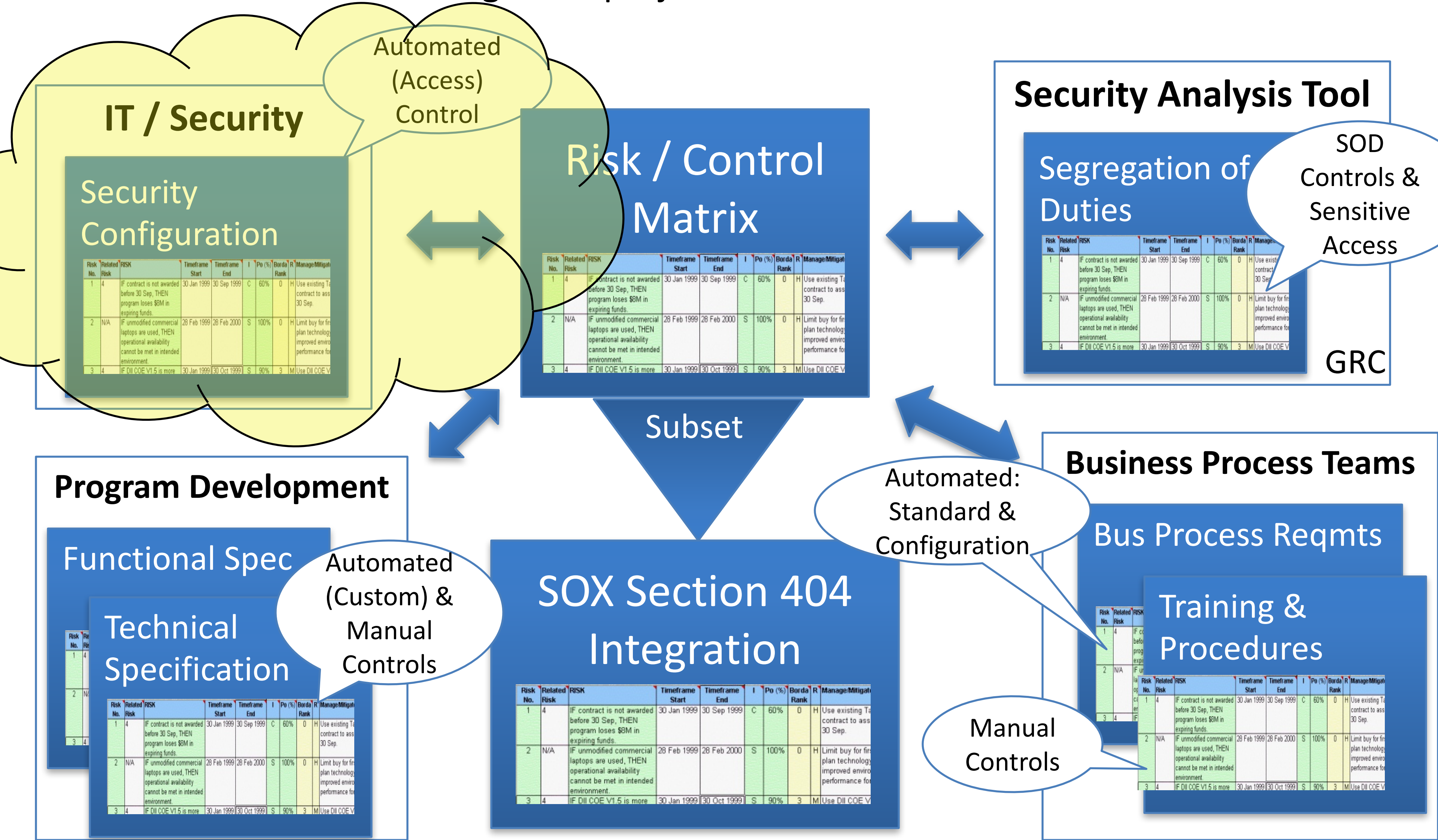
Risk/Control Matrix can serve as the primary vehicle for integrating control design into project activities and deliverables



Risk No.	Related Risk	RISK	Timeframe Start	Timeframe End	I	Po (%)	Borda Rank	R	Manage/Mitigat
1	4	IF contract is not awarded before 30 Sep, THEN program loses $8M in expiring funds.	30 Jan 1999	30 Sep 1999	C	60%	0	H	Use existing Ta contract to ass 30 Sep.
2	N/A	IF unmodified commercial laptops are used, THEN operational availability cannot be met in intended environment.	28 Feb 1999	28 Feb 2000	S	100%	0	H	Limit buy for firs plan technology improved enviro performance for
3	4	IF DII COE V1.5 is more	30 Jan 1999	30 Oct 1999	S	90%	3	M	Use DII COE V

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

Security Analysis Tool

Segregation of Duties

SOD Controls & Sensitive Access

GRC

Subset

SOX Section 404 Integration

Program Development

Functional Spec

Technical Specification

Automated (Custom) & Manual Controls

Business Process Teams

Bus Process Reqmts

Training & Procedures

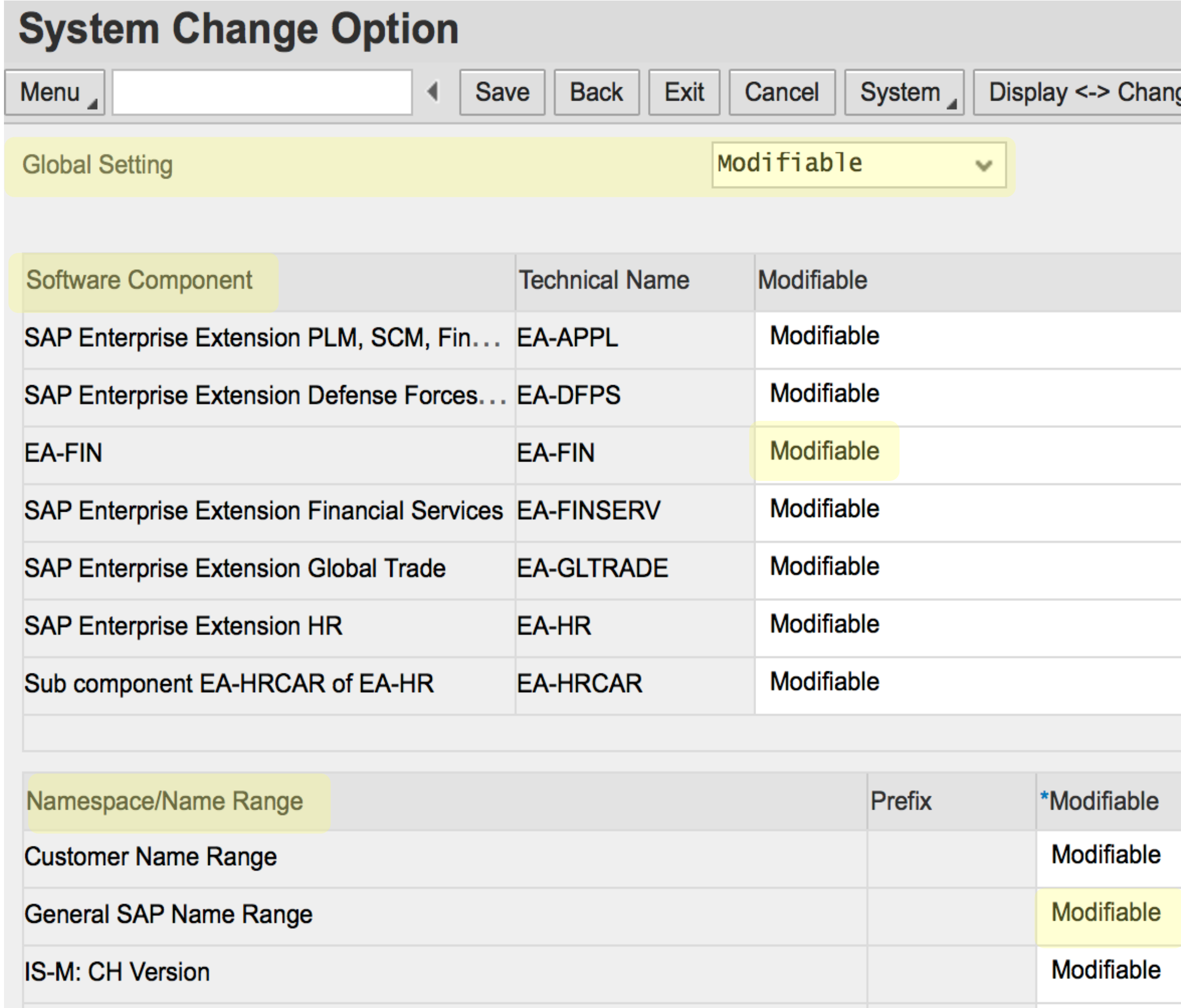
Automated: Standard & Configuration

Manual Controls

Risk No.	Related Risk	RISK	Timeframe Start	Timeframe End	I	Po (%)	Borda Rank	R	Manage/Mitigat
1	4	IF contract is not awarded before 30 Sep, THEN program loses $8M in expiring funds.	30 Jan 1999	30 Sep 1999	C	60%	0	H	Use existing Ta contract to ass 30 Sep.
2	N/A	IF unmodified commercial laptops are used, THEN operational availability cannot be met in intended environment.	28 Feb 1999	28 Feb 2000	S	100%	0	H	Limit buy for fir plan technology improved enviro performance fo
3	4	IF DII COE V1.5 is more	30 Jan 1999	30 Oct 1999	S	90%	3	M	Use DII COE V

Setting System Change Options

- Client Independent Object Modifiable if these parameters are ‘Modifiable’
  - Global Setting
  - Software component of object
  - Namespace or Name Range



System Change Option

Global Setting: Modifiable

Software Component	Technical Name	Modifiable
SAP Enterprise Extension PLM, SCM, Fin...	EA-APPL	Modifiable
SAP Enterprise Extension Defense Forces...	EA-DFPS	Modifiable
EA-FIN	EA-FIN	Modifiable
SAP Enterprise Extension Financial Services	EA-FINSERV	Modifiable
SAP Enterprise Extension Global Trade	EA-GLTRADE	Modifiable
SAP Enterprise Extension HR	EA-HR	Modifiable
Sub component EA-HRCAR of EA-HR	EA-HRCAR	Modifiable

Namespace/Name Range	Prefix	*Modifiable
Customer Name Range		Modifiable
General SAP Name Range		Modifiable
IS-M: CH Version		Modifiable

Setting System Change Options

- Transaction: SE06

		Software Component		
		Modifiable	Restricted	Not Modifiable
Namespace	Modifiable	Existing Objects can be changed	Existing objects can be repaired	
		New objects have SAP System ID of original System	New objects have SAP System ID of original System	
	Not Modifiable	*No Changes Possible*		