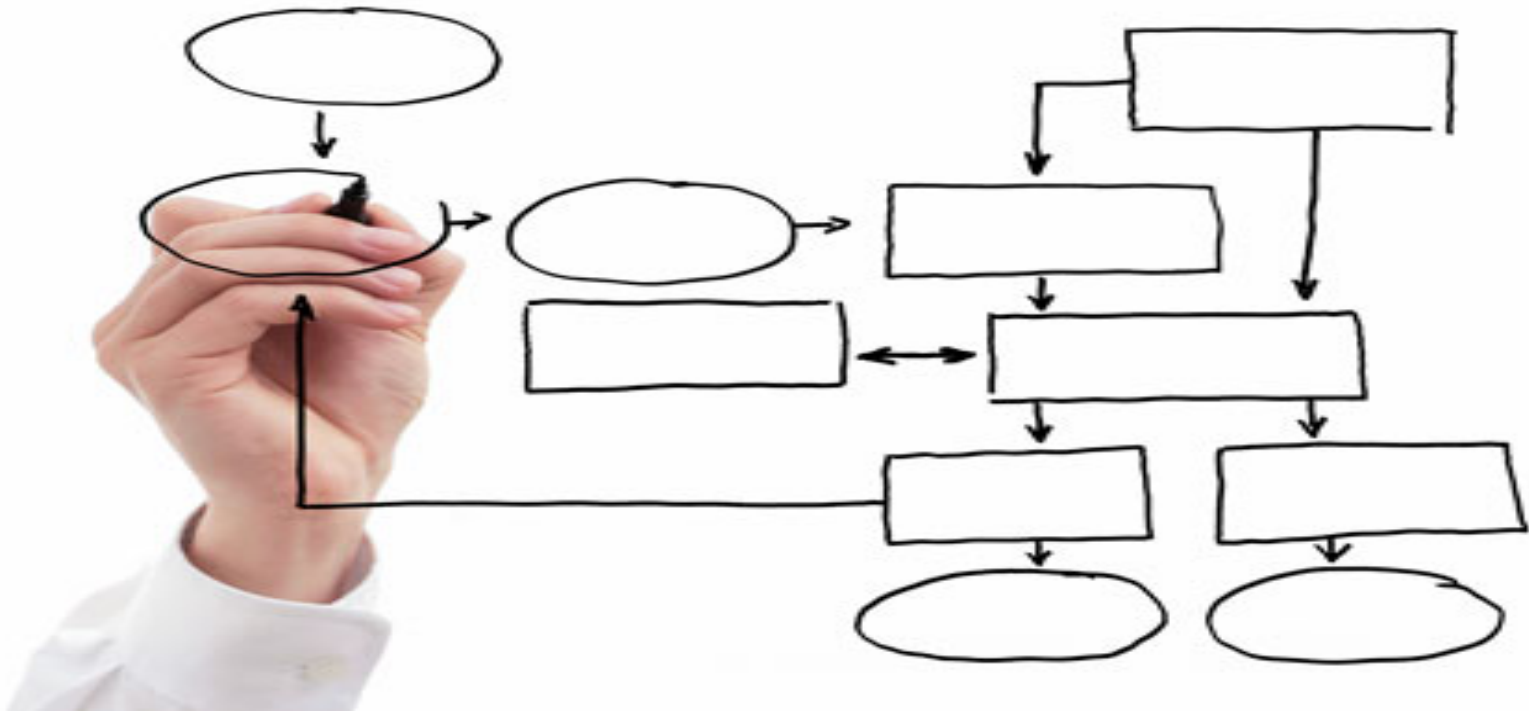


MIS 5121: Business Processes, ERP Systems & Controls
Week 11: *Change Management, IT Controls Framework*



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: Anthony Lucas

Control Failure: Ball State University

- **Background:**

- ❖ Ball State University located in Muncie, Indiana was the subject of \$13.1 million investment fraud scam
- ❖ This was the second time in five years
- ❖ Hired Gale Prizevoits as the Director for Cash and Investments

- **Control Failures:**

- ❖ The director of Cash and Investments for the university issued 3 contracts to a fraudulent investor on her own.
- ❖ 5.047²⁷ % Interest rate on a \$3 million investment is abnormal due to rates having no more than 3 digits after the decimal
- ❖ Different code numbers were used to identify the same investment similar to having a duplicate social security number
- ❖ University policy limits investments to 5 years, this investment listed a maturity date of Aug. 27, 2036, on a Fannie Mae investment.
- ❖ Documentation is used to verify the purchase, payments, wire fund transfers and provide confirmation of that purchase. No documentation exists.

- **Results:**

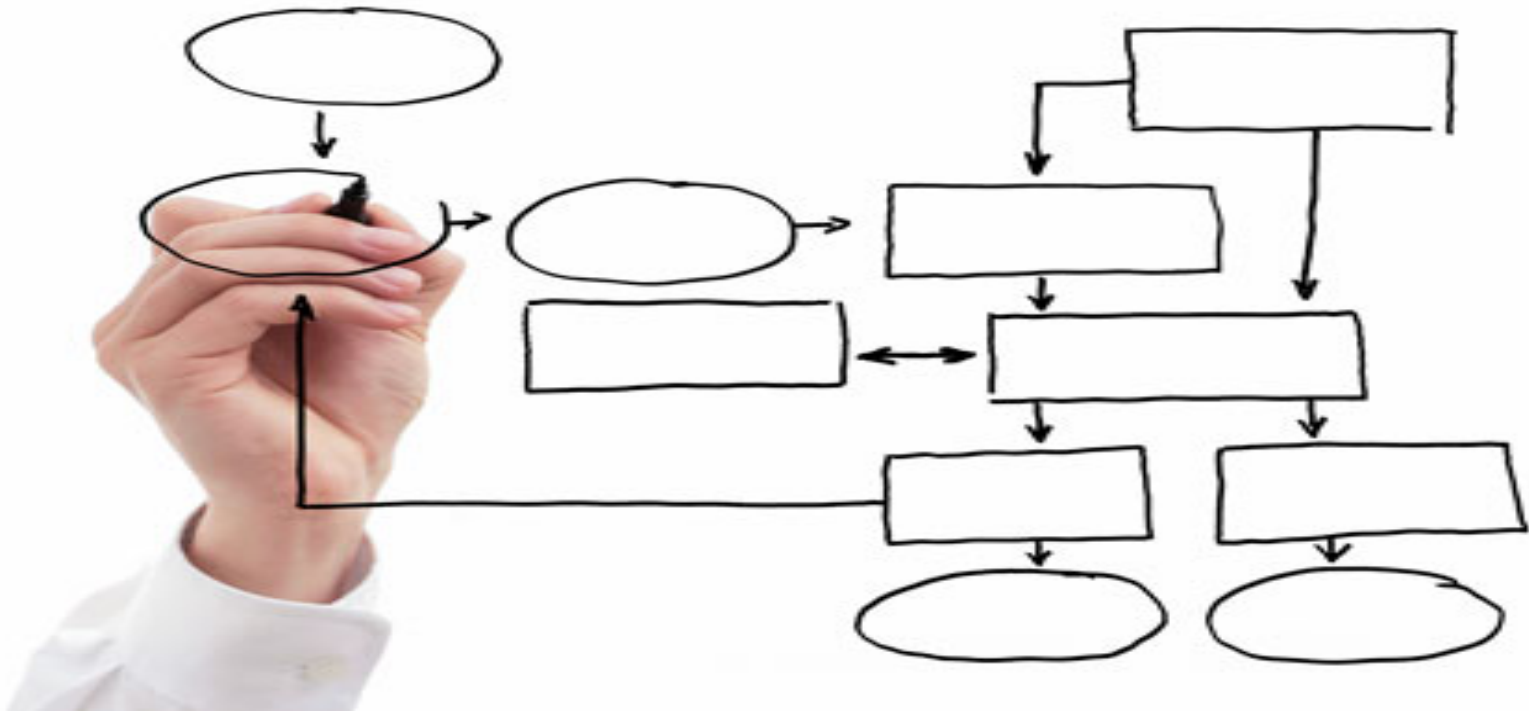
- ❖ Seven people linked to scandal have now been either convicted, disbarred, sued for fraud or gone bankrupt.
- ❖ The university was able to recover some of the loses through lawsuits.
- ❖ University wrote off \$2.9 million of the \$13.1 million lost
- ❖ Case is ongoing
- ❖ An internal control audit has been scheduled to strengthen the control and mitigate future fraud.

- **What Could / Should those in Authority Have Done Different?:**

- ❖ Perform a background check on the Director who had a history of attempted fraud in the state.
- ❖ Create a approved investor list subject to periodic review.
- ❖ Established a dual approval system for all investments

Control Failure: Ball State University

- Reference:
 - ❖ [ball-state-fraud-involved-failed-internal-controls](#)
 - ❖ [Rabbi Linked To Ball State University \(IN\) Fraud | The Ugly Truth](#)
 - ❖ [Ball State records: Deception or lack of due diligence?](#)
 - ❖ [Home - Ball State University](#)



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures: Target

By: Mengyuan Wang



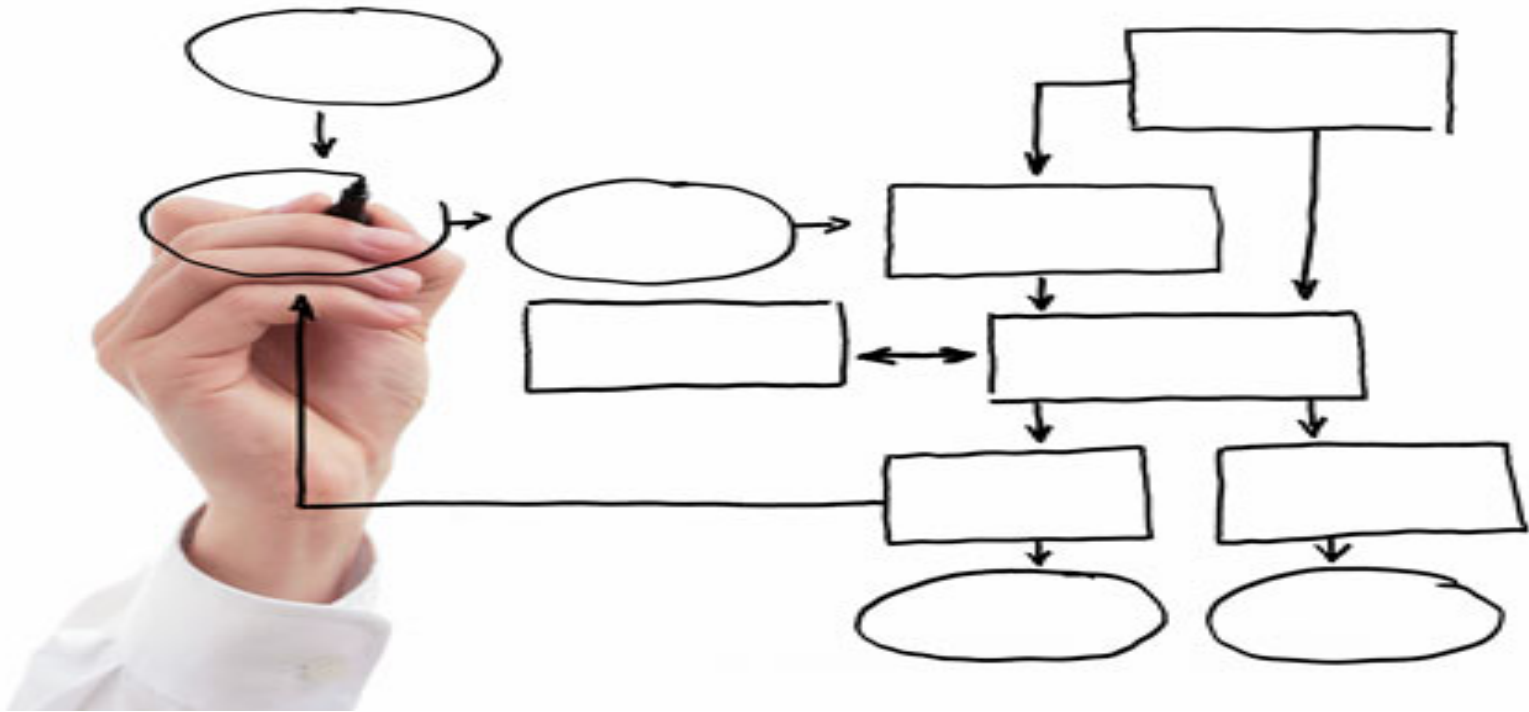
Control Failure: Target

- Background:
 - ❖ Target Corporation is the second-largest discount retailer in the United States
 - ❖ In December 2013 over 40 million credit cards were stolen from nearly 2000 Target stores by accessing data on POS systems
- Control Failures:
 - ❖ Target gave network access to a third-party vendor, a small Pennsylvania HVAC company
 - ❖ Target failed to respond to multiple automated warnings from the company's anti-intrusion software
 - ❖ Network segregation was lacking
 - ❖ Target failed to properly isolate its most sensitive network assets.
- Results:
 - ❖ Vendors were subject to phishing attacks
 - ❖ The attackers were installing malware on Target's system
 - ❖ While the attack was in progress, monitoring software alerted staff in India. They in turn notified Target staff in Minneapolis but no action was taken
 - ❖ Credit cards information were then sold on the black market



Control Failure: Target

- What Could / Should those in Authority Have Done Different?:
 - ❖ Use security awareness training to make employees aware of the danger of sharing too much information.
 - ❖ Remove vendor information and Microsoft case study with detailed information about Target technical systems, processes and staff. Network access could restrict access to vendor and technical information.
 - ❖ Require vendors to use commercial virus checking software and other security precautions on the systems used to interact with vendor portals.
 - ❖ Require vendors to go through basic security training or agree to train staff.
- Reference:
 - ❖ <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412>
 - ❖ https://en.wikipedia.org/wiki/Target_Corporation
 - ❖ https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiVIYPq_ujLAhVmulMKHaG9AvUQFggiMAE&url=http%3A%2F%2Fdocs.ismgcorp.com%2Ffiles%2Fexternal%2FTarget_Kill_Chain_Analysis_FINAL.pdf&usq=AFQjCNF8h1j5XmbVgYd13RkxdWvTw8dJYA&bvm=bv.118353311,d.dmo



MIS 5121: Business Process, ERP Systems & Controls

Real World Control Failures:

By: Shiting Liu

Control Failure: American Insurance Group

- Background:
 - ❖ Multination Insurance Corporation & Largest U.S. commercial insurer
 - ❖ 93,000 employees & 130 countries
 - ❖ World's biggest reinsurance buyer

- Control Failures:
 - ❖ Recorded loans as revenue: \$500M loan from Gen Re.
 - ❖ Recorded the amount to reserve funds used to pay potential claims
 - ❖ Hid losses in financial statements
 - ❖ Didn't record deferred acquisition costs in a timely manner
 - ❖ Paid insurance brokers to steer business to AIG
 - ❖ Used collateral to buy mortgage backed securities

- Results:
 - ❖ Greenberg forced to step down as CEO but has faced no criminal charges
 - ❖ AIG settled case for 1.6 billion
 - ❖ 16 counts of alleged violation of criminal code

What Could / Should those in Authority Have Done Different?:

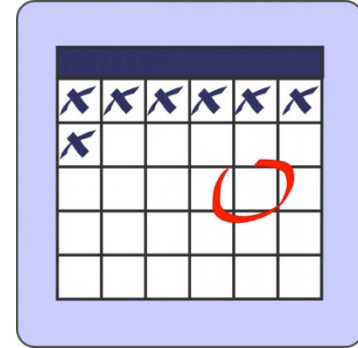
- ❖ Engage in Ethical Behaviors
- ❖ Improve transparency
- ❖ Taxpayer protections need to be institutionalized at the outset

Reference:

- ❖ Accounting Fraud: <http://www.bloomberg.com/news/articles/2005-04-10/aig-what-went-wrong>
- ❖ <http://www.usnews.com/news/blogs/rick-newman/2012/12/11/3-lessons-from-the-aig-bailout>



MIS 5121: Upcoming Events



- **Exam 2** – In class: *April 4 (today)*
- Reading Assignment 7 – *Due: April 10*
- 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

- _____
- _____
- _____
- _____
- _____
- _____

Change Management

SAP: Transport Management

Key Information Technology Risks

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



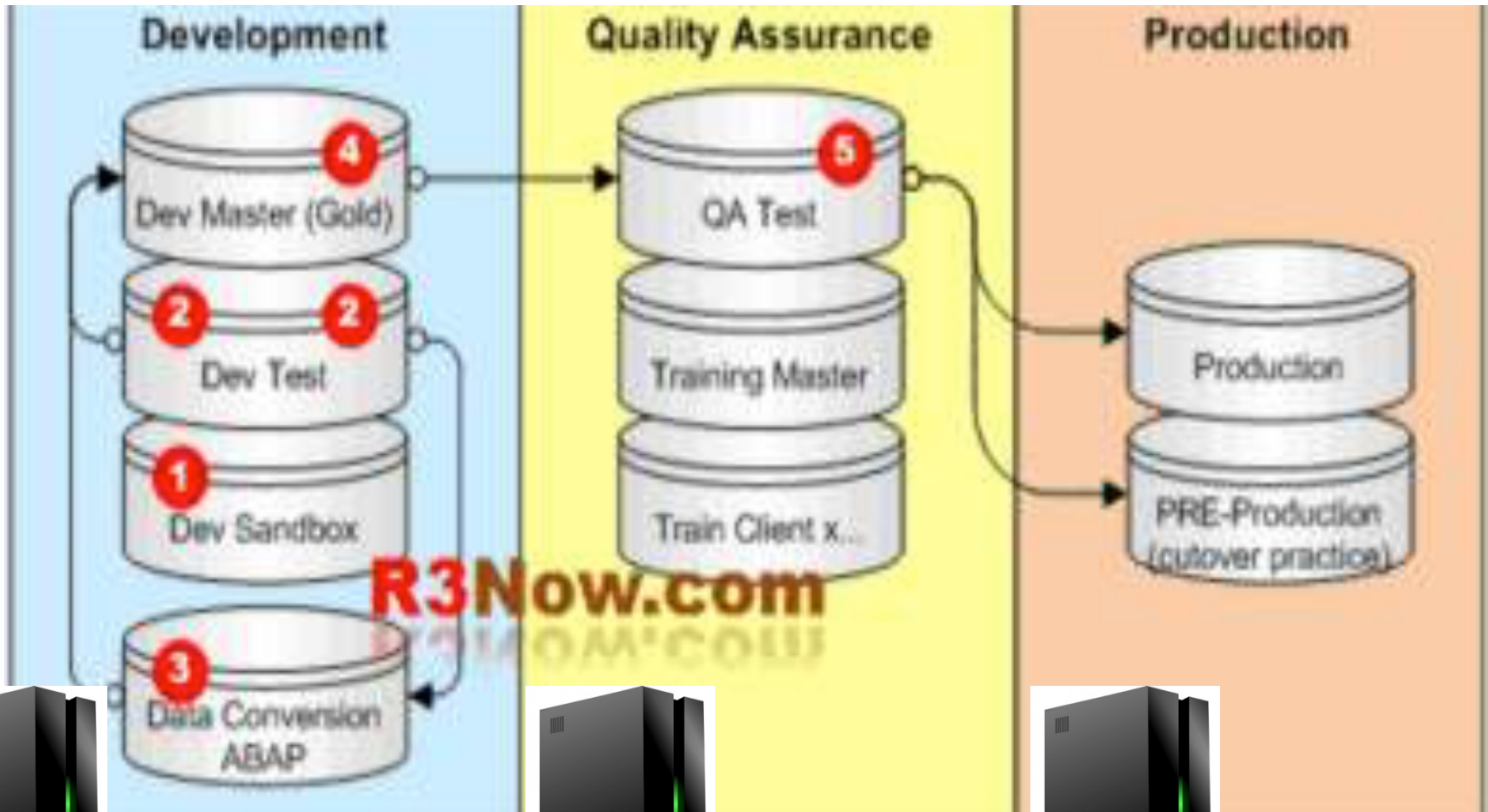
SAP Landscape: Instance and Clients

- **SAP Instance**

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



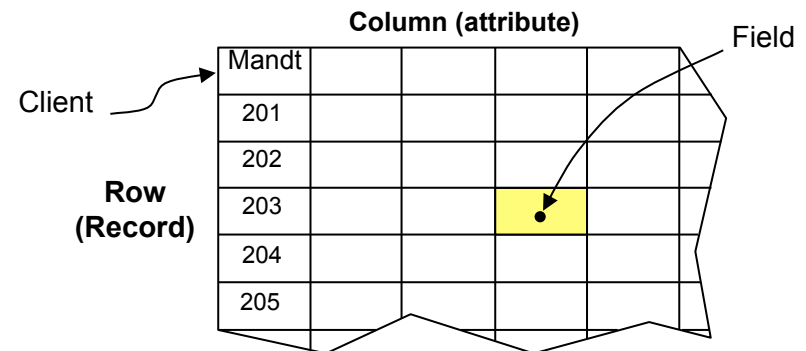
Minimum Rec'd SAP Landscape



SAP Landscape: Instance and Clients

- **SAP Clients**

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



Typical SAP Landscape

Development System

Type of Users:

-
-
-

Type of Work:

-
-
-

Quality-Assurance System

Type of Users:

-
-
-

Type of Work:

-
-
-

Production System

Type of Users:

-
-
-

Type of Work:

-
-
-



Typical SAP Landscape

Development System

Type of users:
Developers,
Consultants,
Key Users

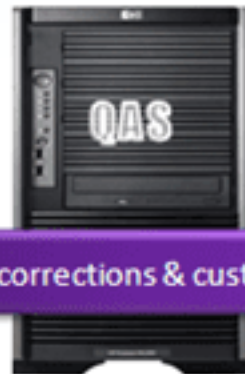
Type of work:
Customizing,
Development,
Unit Testing



Quality-Assurance System

Type of users:
Developers,
Consultants,
Key Users

Type of work:
Integration and
Quality testing



Production System

Type of users:
End users

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



Developments, corrections & customizing settings

Client Dependent vs. Independent

System/Instance

Client Dependent

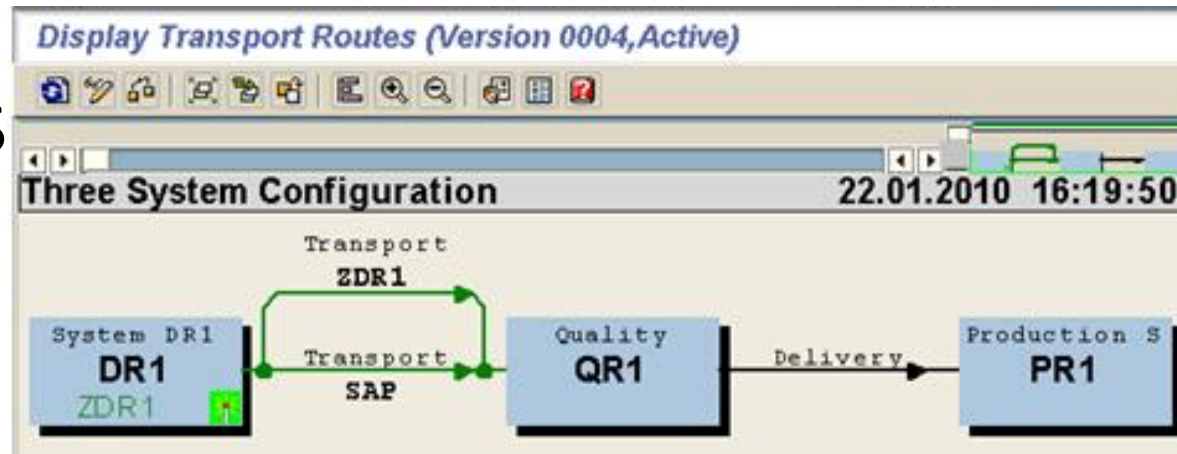
Dev 100 Master (Gold)	Dev 110 Dev Test	Dev 180 Data Conversion	Dev 900 Sandbox
<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data	<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data	<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data	<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data

Client Independent

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

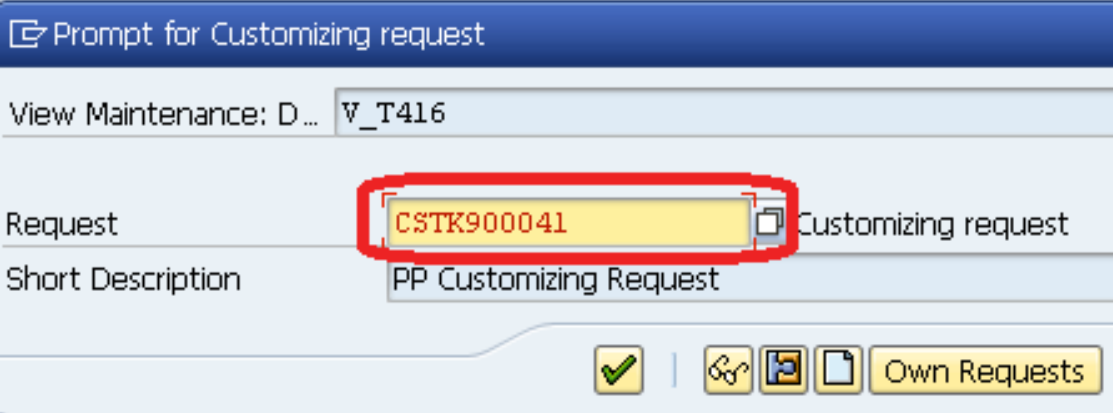
SAP Change Management

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



SAP Change Management

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



Prompt for Customizing request

View Maintenance: D... V_T416

Request	CSTK900041	Customizing request
Short Description	PP Customizing Request	

Own Requests

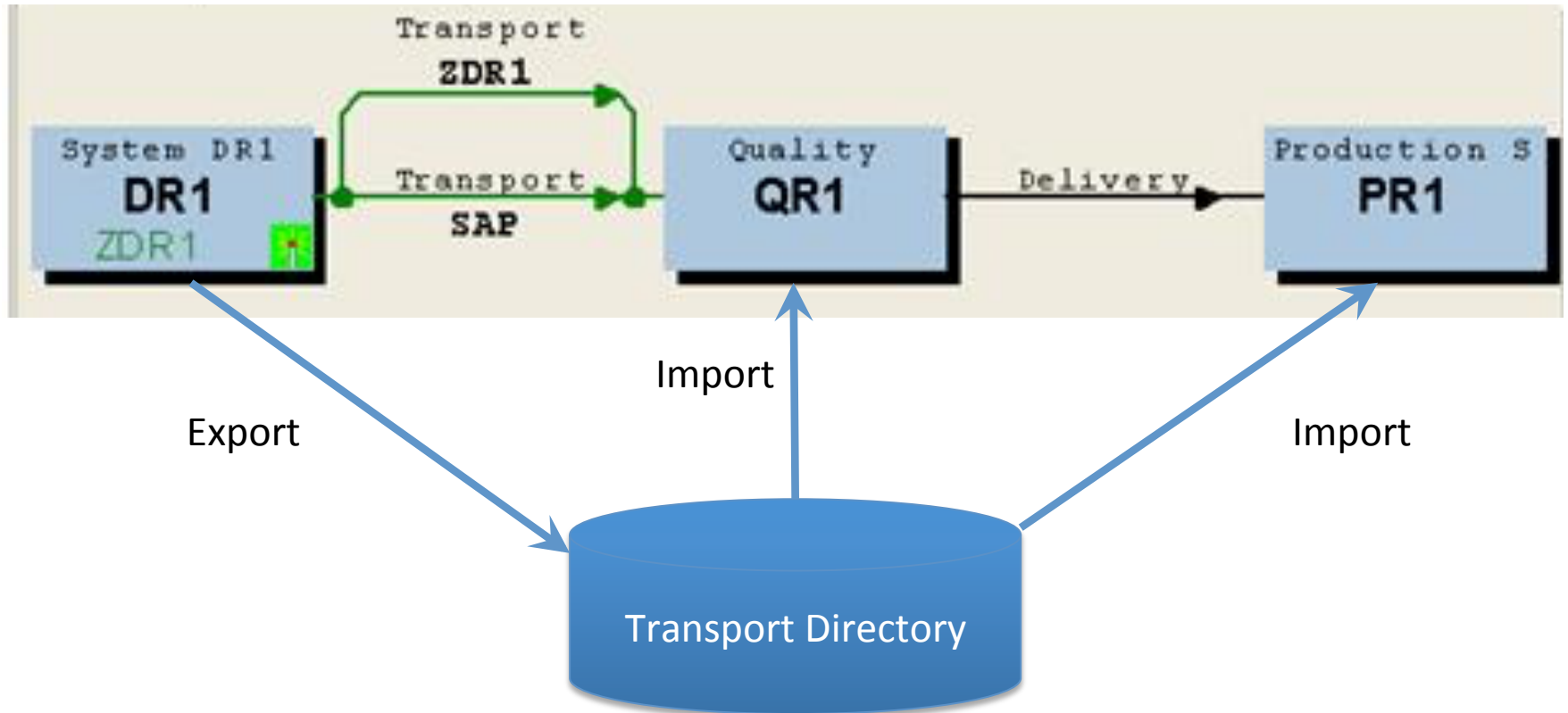


TMS Terminology

- 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 Process

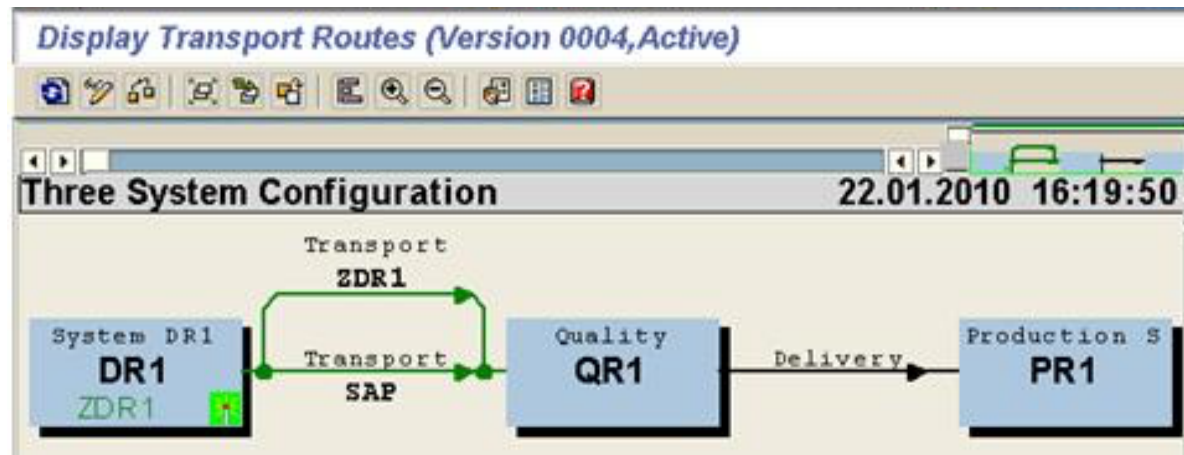


Note: For any given change, the **same** change is moved / migrated to **each** system. Changes are not moved from system to system.



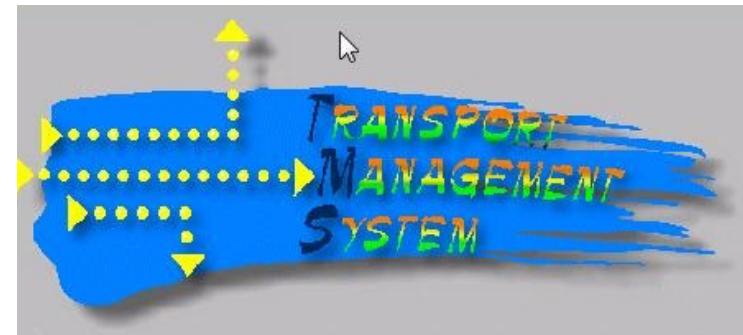
Transport Paths

- 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



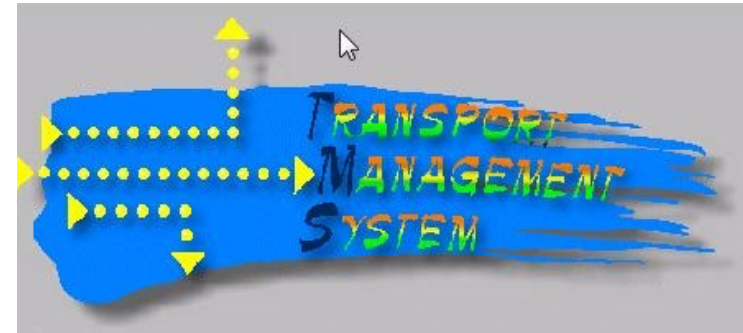
Transport Process

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



Transport Security

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



Transport Controls

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



SAP Landscape: Instance Security

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



Critical Instance Profile Parameters



Parameter / Description	SAP Default	Recommended
<i>Login/min_password_lng</i> Minimum password length	3	5
<i>Login/min_password_lng</i> # days after which password must change	0	30-60 Days
<i>Login/fails_to_session_end</i> # times bad password to end session	3	3
<i>Login/fails_to_user_lock</i> # times bad password to lock out	12	3
<i>Login/failed_user_auto_unlock</i> Auto unlock of user at midnight	1 (Auto unlock)	0 (remains locked)

Critical Instance Profile Parameters

Parameter / Description	SAP Default	Recommended
<i>Auth/rgc_authority_check</i> Check authorization for remote function calls (Client/system to other)	0	1 (RFC's are checked)
<i>Rdisp/gui_auto_logout</i> # seconds to auto disconnect inactive users	0	3600
<i>Login/disable_multi_gui_Login</i> Block multi logon if set to 1	0	1



Setting System Change Options

- Transaction: SE06
- Changes affect entire system / instance
- Affects Client Independent objects
- **PRD Global setting should be 'Not Modifiable'**



System Change Option

Menu ◀ Save Back Exit Cancel System ▶ Display <-> Change

Global Setting ▼

Software Component	Technical Name	Modifiable
SAP Enterprise Extension PLM, SCM, Fin...	EA-APPL	Modifiable
SAP Enterprise Extension Defense Equipm...	EA-DEPS	Modifiable

Risk and Recommendation

Instance Profile Parameters

Risks:

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

Recommendations:

Review all parameter values different than recommended – understand why company has chosen non-recommended value



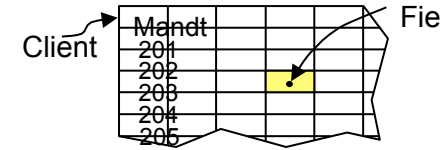
PRD (Production) Instance Security

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



Setting System Security: Clients

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

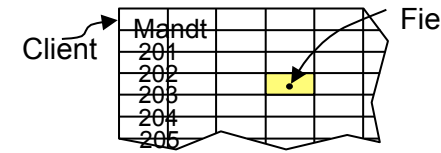


Display View "Clients": C

Menu ◀ ▶ E

Client	Name
000	SAP AG
001	Auslieferungsmandant R11
066	EarlyWatch
300	GBI 2.30 Config (896)
301	GBI 2.30 Config (896)
302	GBI 2.30 Config (896)
303	GBI 2.30 Config (896)
304	GBI 2.30 Config (896)
305	GBI 2.30 Config (896)

Setting System (Client) Security



Std currency: USD

Client role: Training/Education

Recd: 'No Changes Allowed' in PRD to prevent unauthorized changes to Client-specific objects

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

Recd: Level 1 or 2 in PRD to prevent overwriting when using client copy or client comparison tools

Changes and Transports for Client-Specific Objects

- Changes without automatic recording
- Automatic recording of changes
- No changes allowed
- Changes w/o automatic recording, no transports allowed

Cross-Client Object Changes

- No changes to cross-client Customizing objects
- Changes to Repository and cross-client Customizing allowed
- No changes to cross-client Customizing objects
- No changes to Repository objects
- No changes to Repository and cross-client Customizing objs

Client Copy and Comparison Tool Protection

- Protection level 0: No restriction
- Protection level 0: No restriction
- Protection level 1: No overwriting
- Protection level 2: No overwriting, no external availability

Change Management / Transport Management Overview

- Client dependent vs. Client independent objects / components
- Transport Process
 - Transports
 - Transport Paths
 - Activities
 - Controls
- Instance / Client Security: Risks & Recommendations



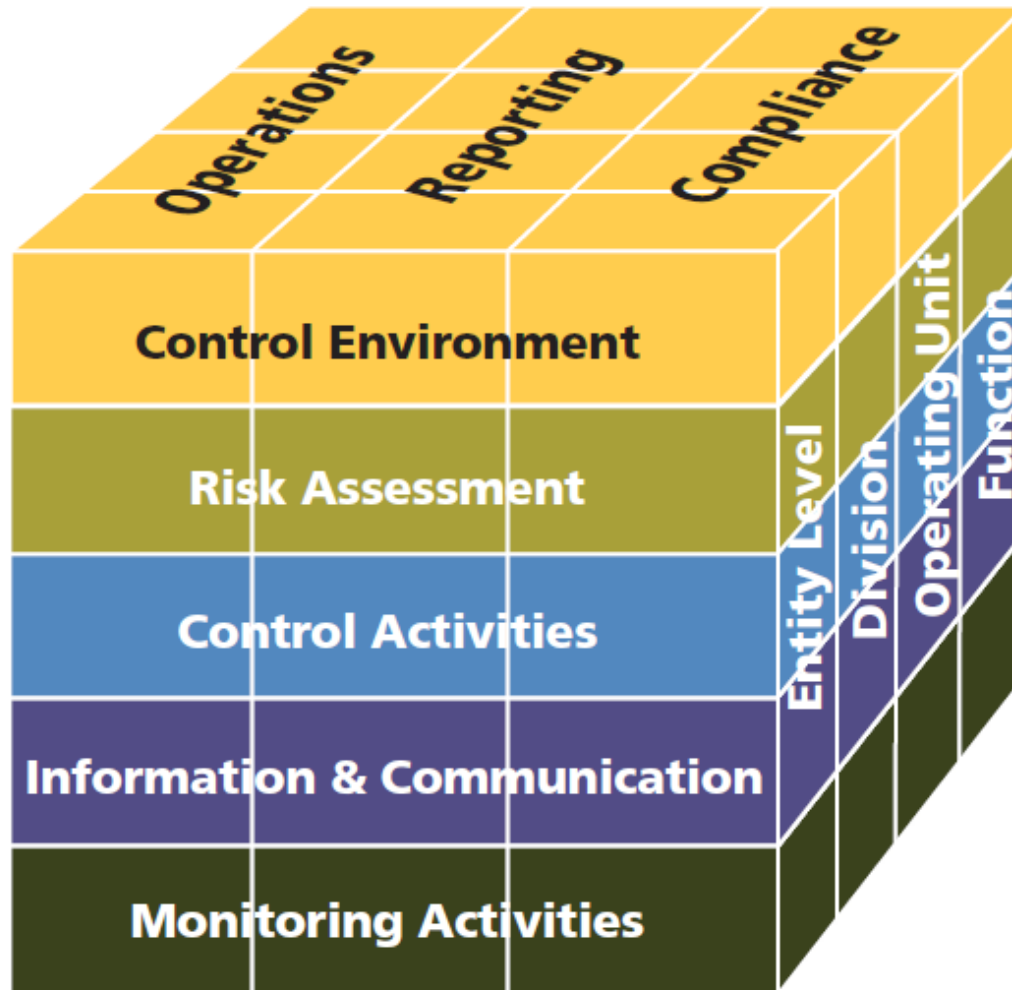
Assignment Questions

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

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

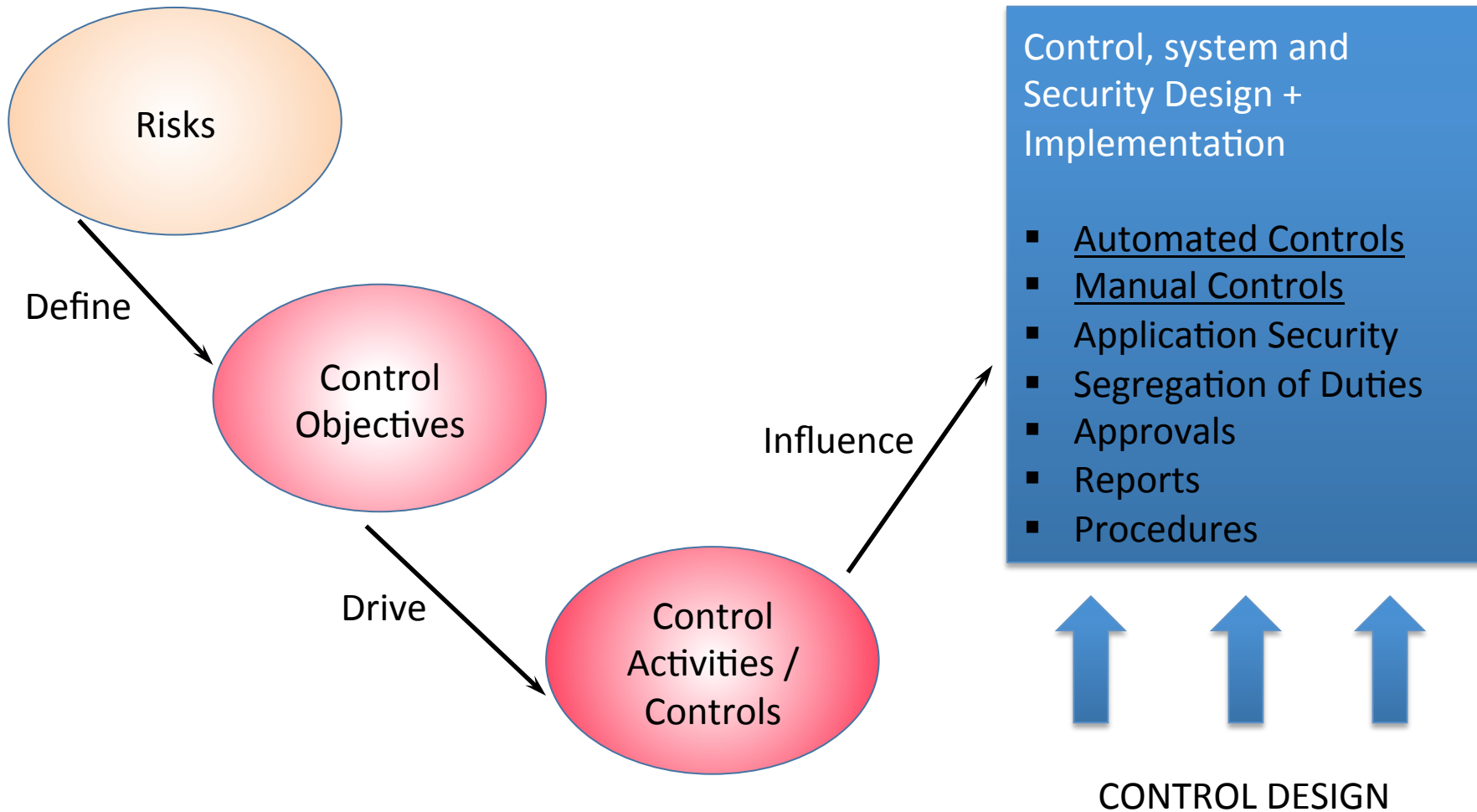
Information & Communication

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





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 (*April 4*): Part 1 (Identify Risks)
 - Future Class (*April 11/18*): Part 2, 3 (Identify Controls, Link Controls to Risks)
 - Future Class (*April 20*): Part 4 (Complete Control Definitions)
 - Future Class (*April 25*): Part 5, 6 (Control Process / Audit Details; Personal Questions)
 - *Due April 28 11:59 PM*: Assignment Submission

Risk / Control Matrix: Final Exercise

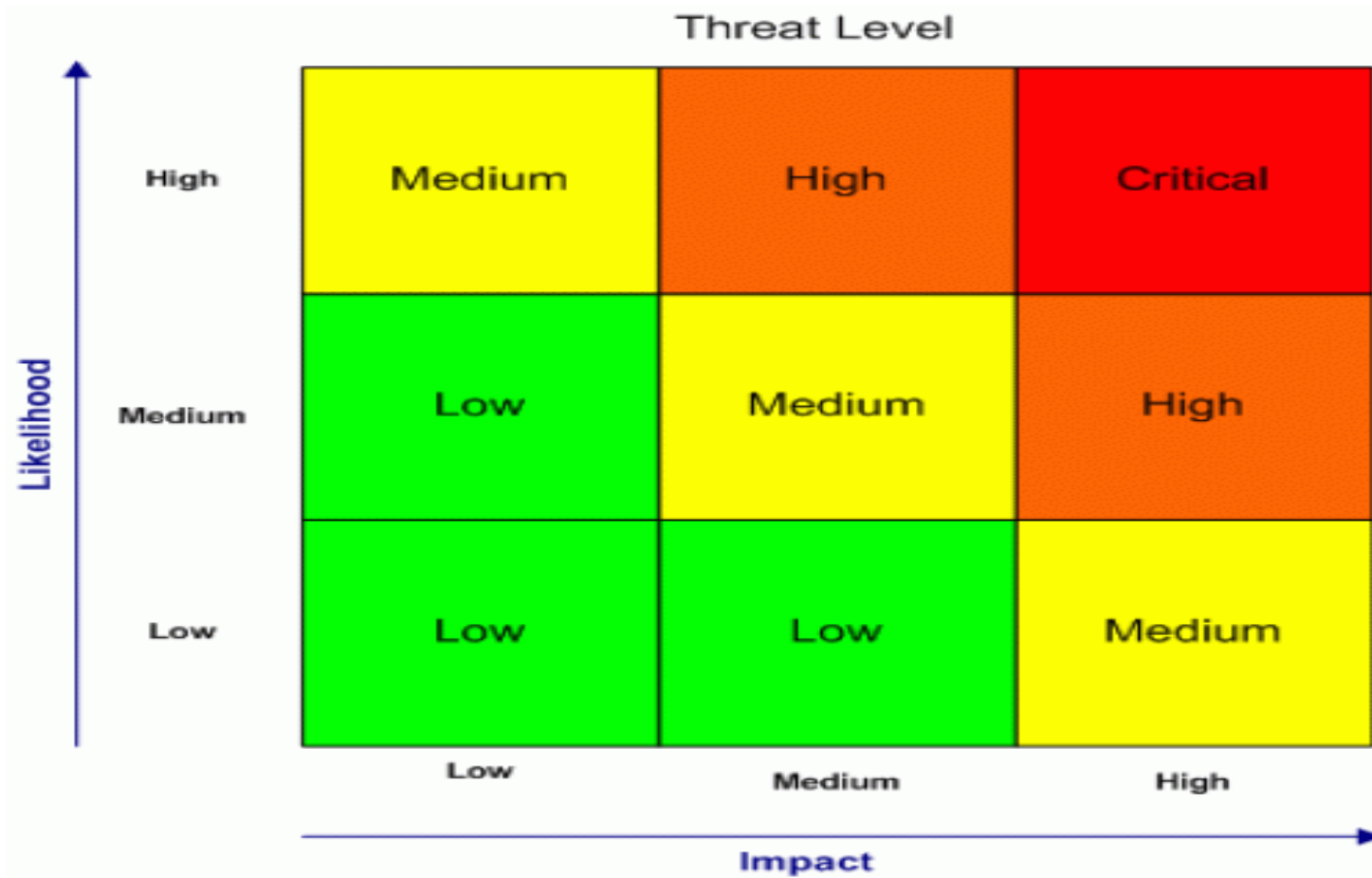


Part 1:

- 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

Extra Slides

Extra Slides



Risk Assessment



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

The screenshot displays the SAP 'Changes in Order 1' interface. At the top, there is a title bar 'Changes in Order 1' and a menu bar with buttons for 'Menu', 'Back', 'Exit', 'Cancel', and 'System'. Below the menu bar is the 'DocHeader' section. The main content area shows a table with the following data:

ID	Time	Sales Promotion	Old value	New value
<input type="checkbox"/>	16:48:45	Incoterms (Part 2) change	Miami	Tampa

Below this table, there is a smaller window titled 'Changes in Order 1' with its own 'DocHeader' section. This window displays a detailed table of the change:

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).

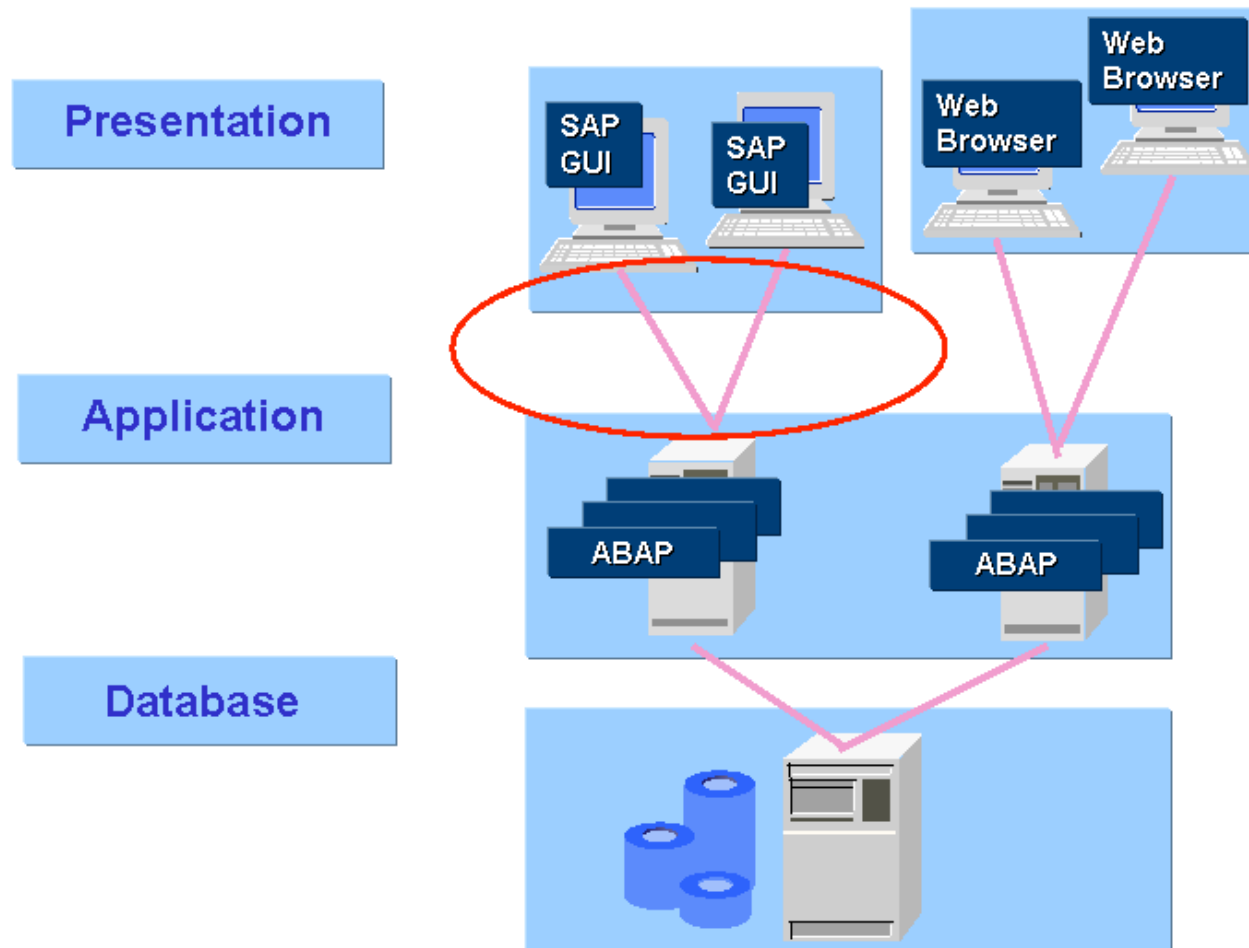
Investigate ways access to maintenance of change documents could be further restricted (locking transaction)

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 Environment



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

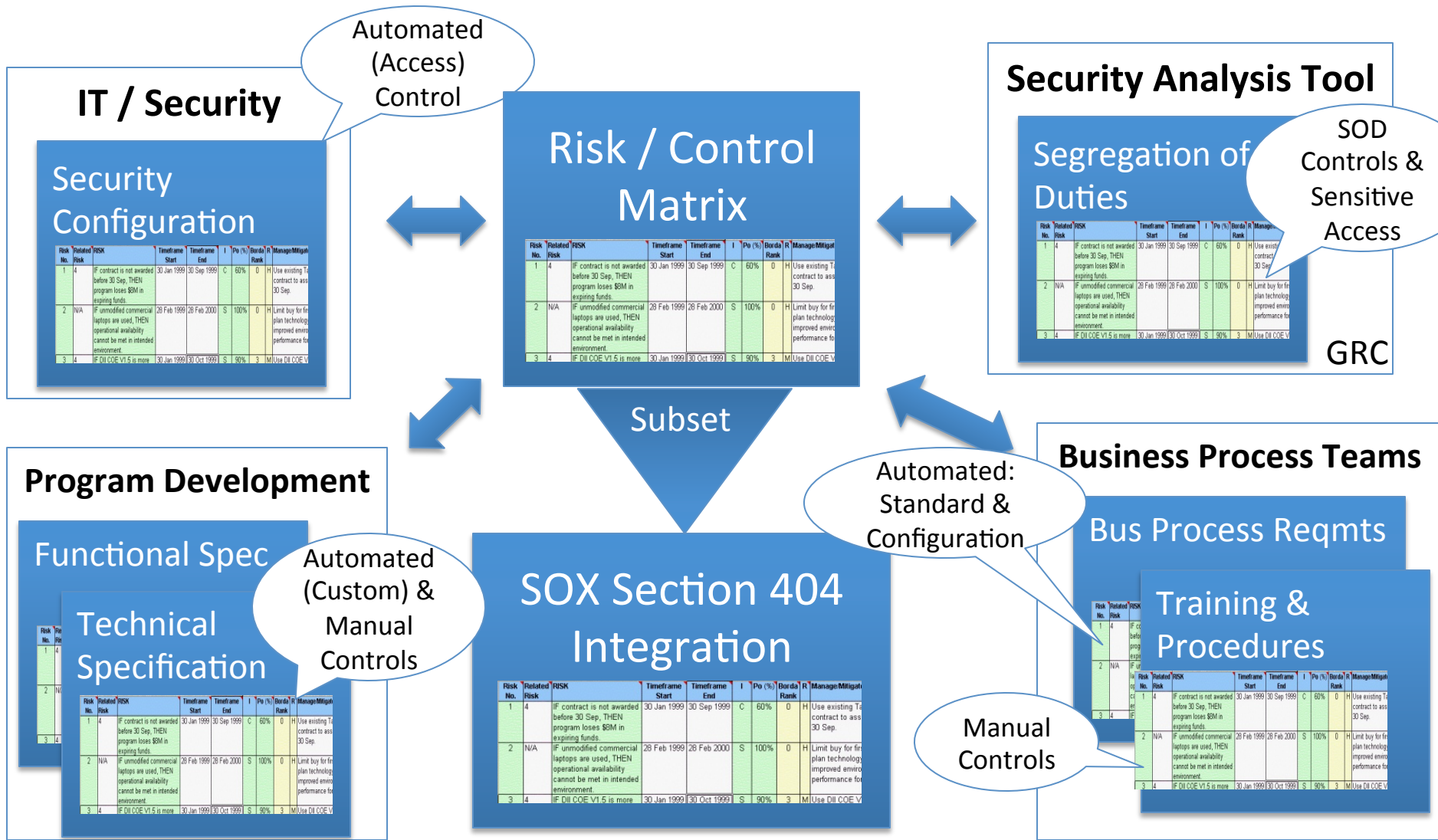
Table Driven System

- 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

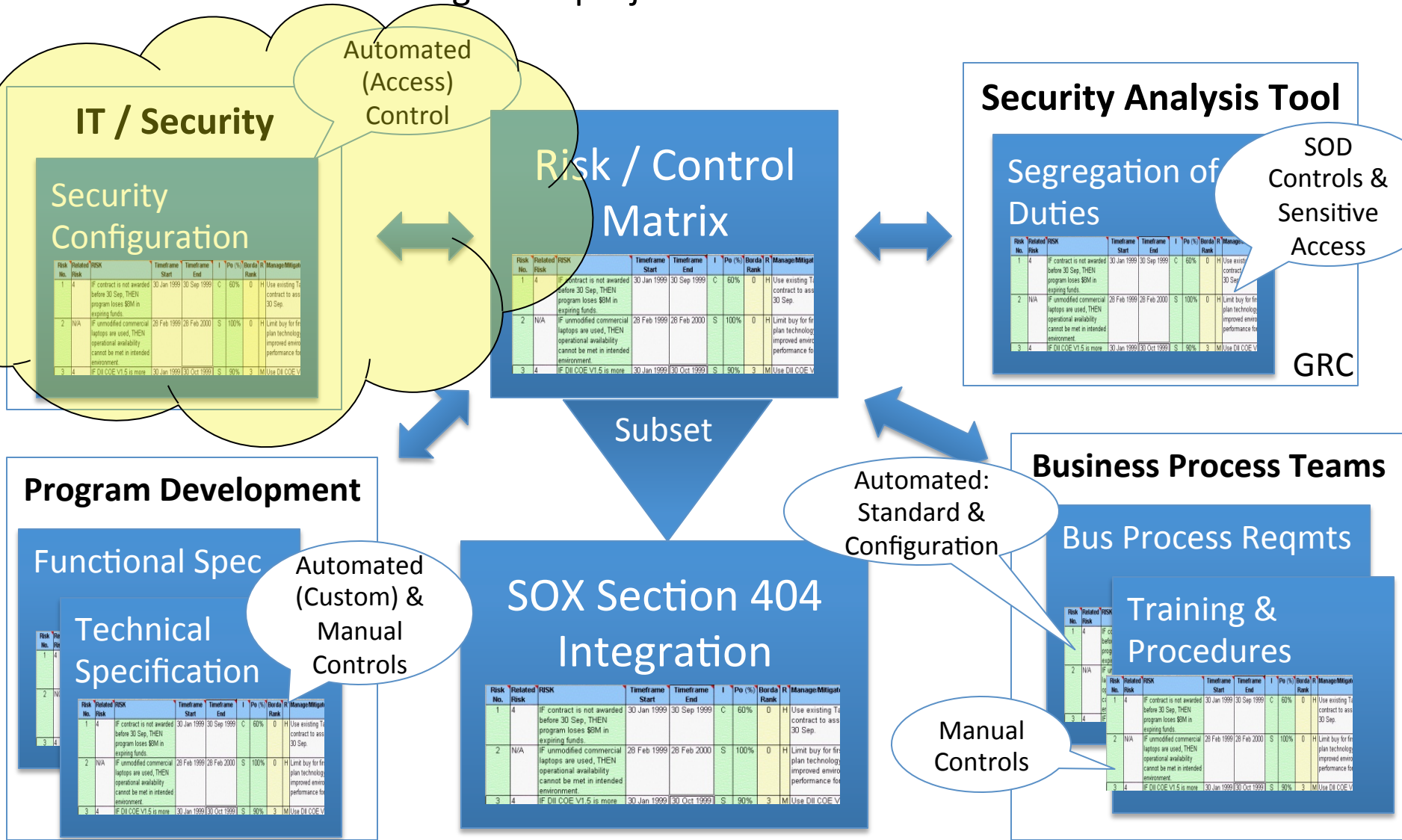
Controls: Integration Points

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



Client Dependent vs. Independent

System/Instance

Client Dependent

Dev 100 Master (Gold)	Dev 110 Dev Test	Dev 180 Data Conversion	Dev 900 Sandbox
<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data	<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data	<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data	<ul style="list-style-type: none">- Master Data- Transaction Data- User Management / Data

Client Independent

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

Setting System Change Options

- Client Independent Object Modifiable if these parameters are 'Modifiable'

– Global Setting

– Software component of object

– Namespace or Name Range

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	
	Modifiable	New objects have SAP System ID of original System	New objects have SAP System ID of original System	
	Not Modifiable	<i>No Changes Possible</i>		