

Auditing in SAP Environment

- CA Shirish PADEY
- Sunit Belapure CISA
- CA Chetan Damle
- CA Gautam Kamat
- CA Sujay Joshi
- CA NirenDesai

ICAI-Pune Branch
21st June,2015

Agenda

1. Introduction to Controls based Audit
2. Introduction to SAP
3. Accessing and Navigating SAP
4. SAP Organization
5. Review of IT General Controls (Other than BASIS)
6. Review of SAP BASIS
7. Validation of Automated Controls
8. Authorization Concept
9. Segregation of Duties
10. Data Migration to SAP
11. SAP Upgrade
12. Report Validation
13. JE Extraction and Analysis
14. Other Challenges in SAP

SESSION 1

Introduction to Controls based Audit



- *Just When I had found all of Life's Answers*

- *They Changed All The Questions*

1.1 Standards on Auditing

- SA315 – Identifying and Assessing the Risk of Material Misstatement Through Understanding of the Entity and its Environment
 - The auditor shall
 - Obtain understanding of Internal Controls
 - Obtain understanding of Information Systems, including related business processes
 - Obtain understanding of how the entity has responded to risks arising from IT
 - Obtain an understanding of the entity's controls over risk of inaccurate or incomplete recording of transactions in highly automated processing environment
- SA330 – The Auditor's Responses to Assessed Risk
 - The auditor shall
 - Consider effectiveness of General IT Controls

1.2 Accounting in ERPs

- All entries are Journal Entries
- There are NO Primary or Secondary Books of Account – only data stored in Tables

1.3 Difficulty in Substantive Audit for ERPs

- Absence of Printouts
- Voluminous data
- Difficulty in Ledger Scrutiny
- Difficulty in audit of “manual” journal entries

1.4 Alternative?

- Reliance on IT General Controls
 - Relying on Automated Controls and Automated Accounting Procedures
 - Reliance on Reports and System-Dependent Manual Controls
 - Reliance on Underlying Data

SESSION 2

Introduction to SAP

2.1 SAP — What is it?

- SAP is a German multinational software corporation that makes ERP with regional offices in almost 130 countries and has over approx. 291,000 customers in 190 countries.
- In German:
 - Systeme, Anwendungen und Produkte in der Datenverarbeitung
- In English:
 - Systems, Applications and Products in Data Processing
- Founded in Walldorf, Deutschland (Germany), 1972
- Not "Sap" — It is "S - A - P"

2.1 SAP — What is it? [Contd.]

★ Timeline:

1972: SAP AG founded in Germany.

1979: SAP R/2 introduced for mainframe computers.

1992: SAP R/3 released as client-server application.

1996: SAP R/3 became partially Internet enabled.

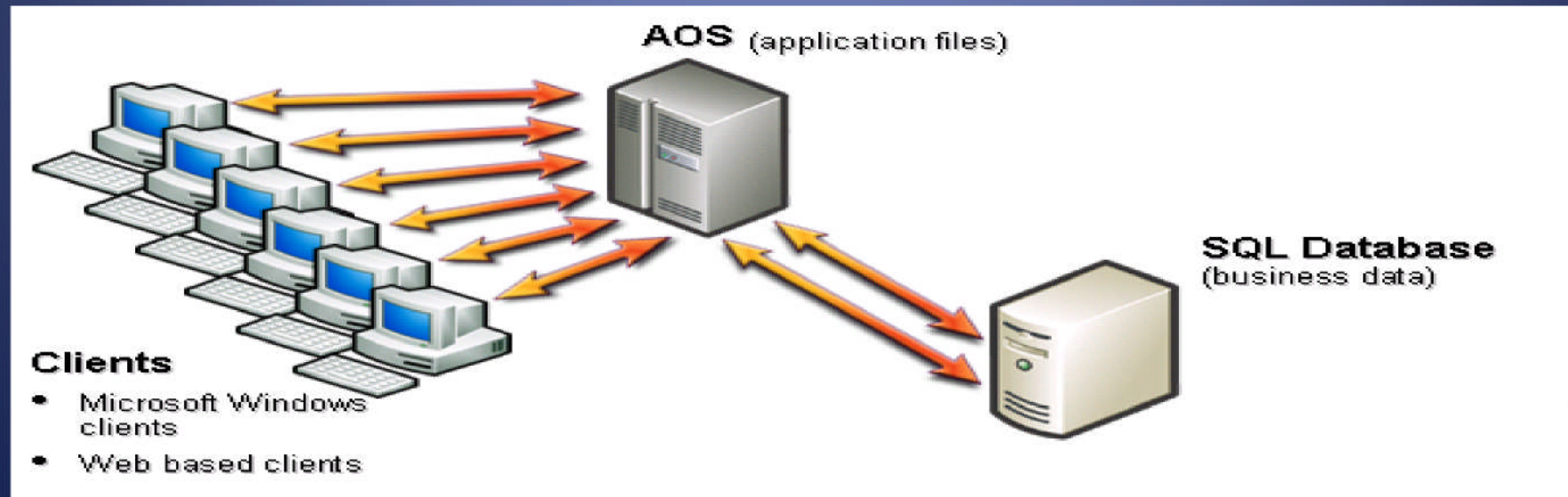
1997: Developed and launched the new dimension product line including CRM, SCM, and Data Warehousing solutions.

1999: SAP announced mySAP.com, the next generation of its Enterprise Application System, based on the Internet architecture.

2000-2005: Introduced mySAP business Suite, NetWeaver, and XApplications.

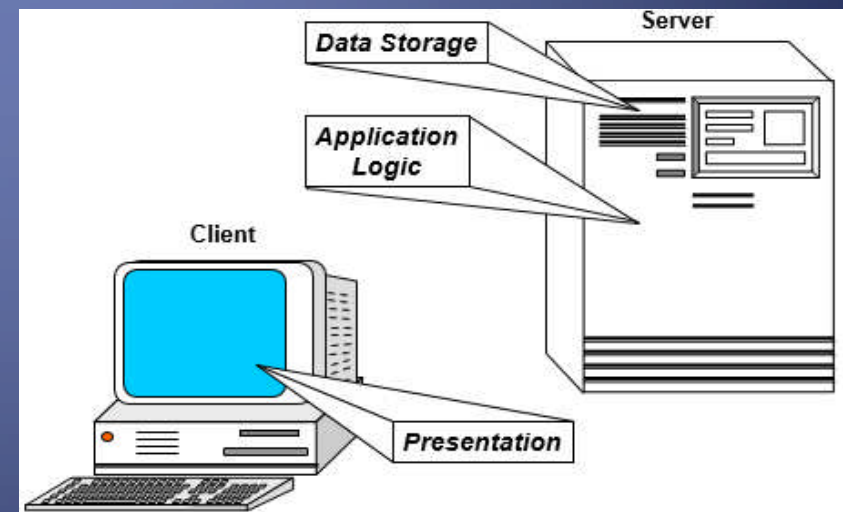
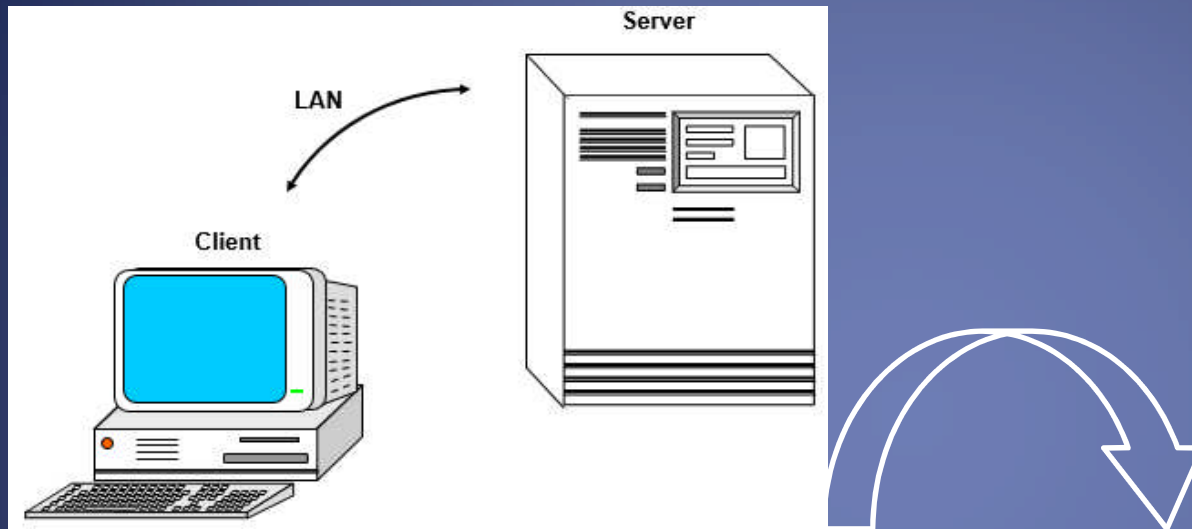
2.2 SAP - The Product

- R/3 — Client — Server (1992)
 - Three tier architecture — Front end (GUI), Application Server, Database Server

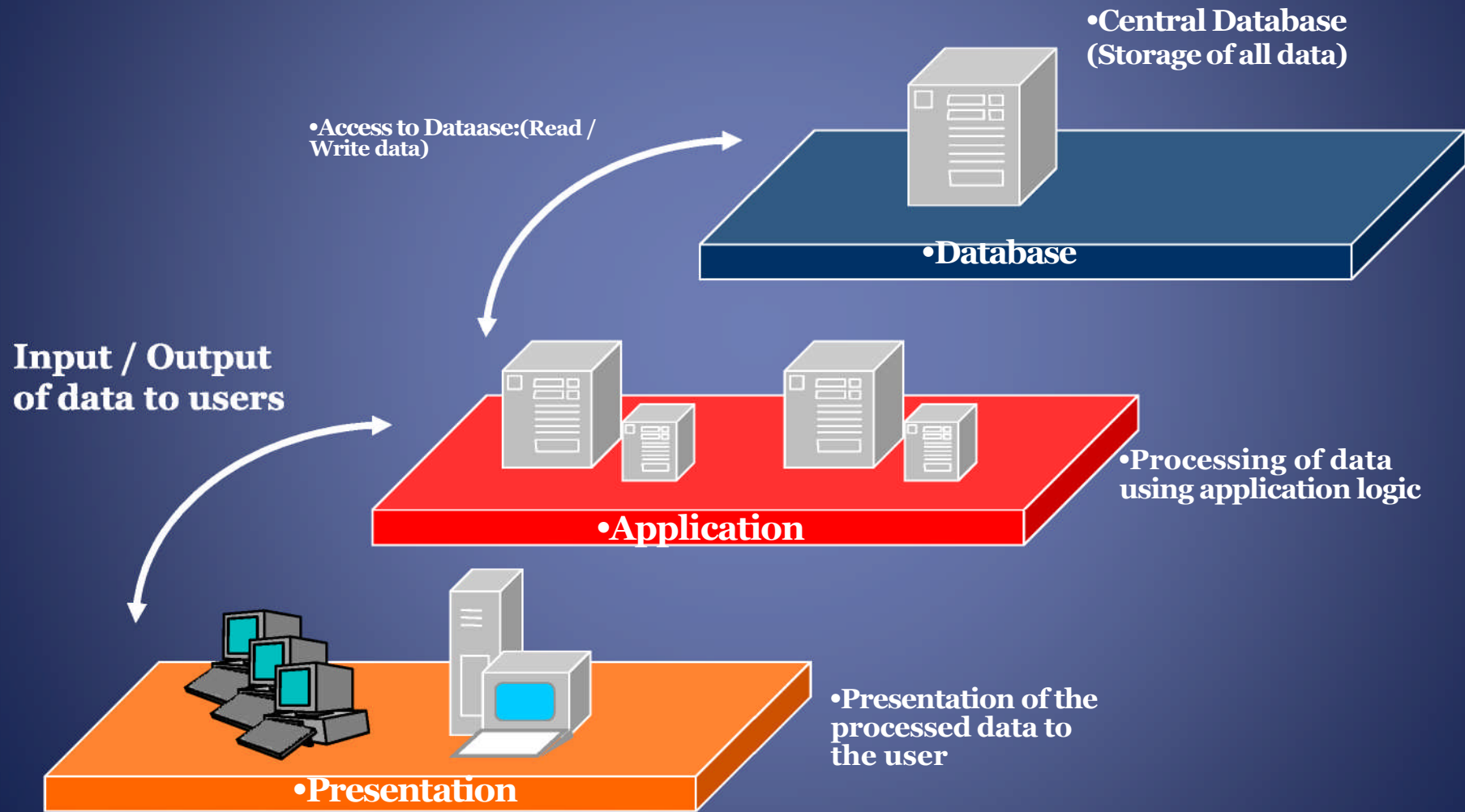


2.2 SAP – The Product [Contd.]

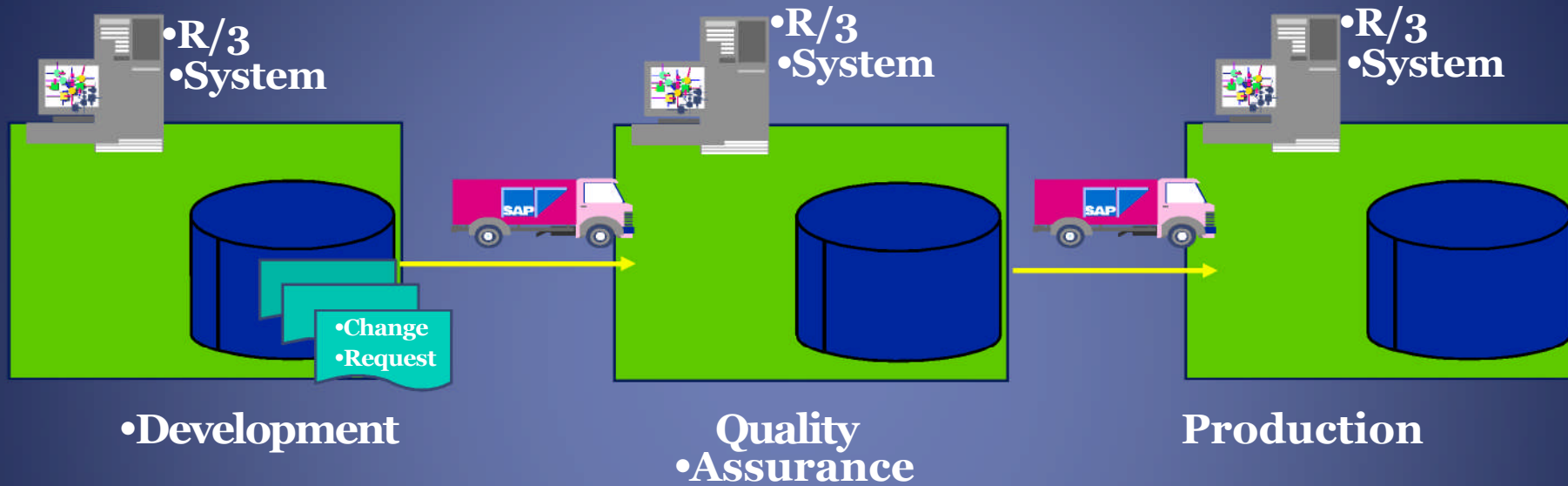
- Client – Server Architecture



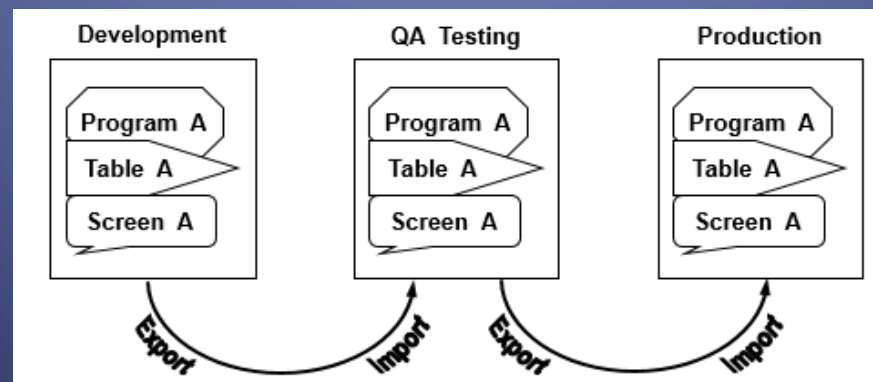
2.3 R/3: Three-Tier Computer



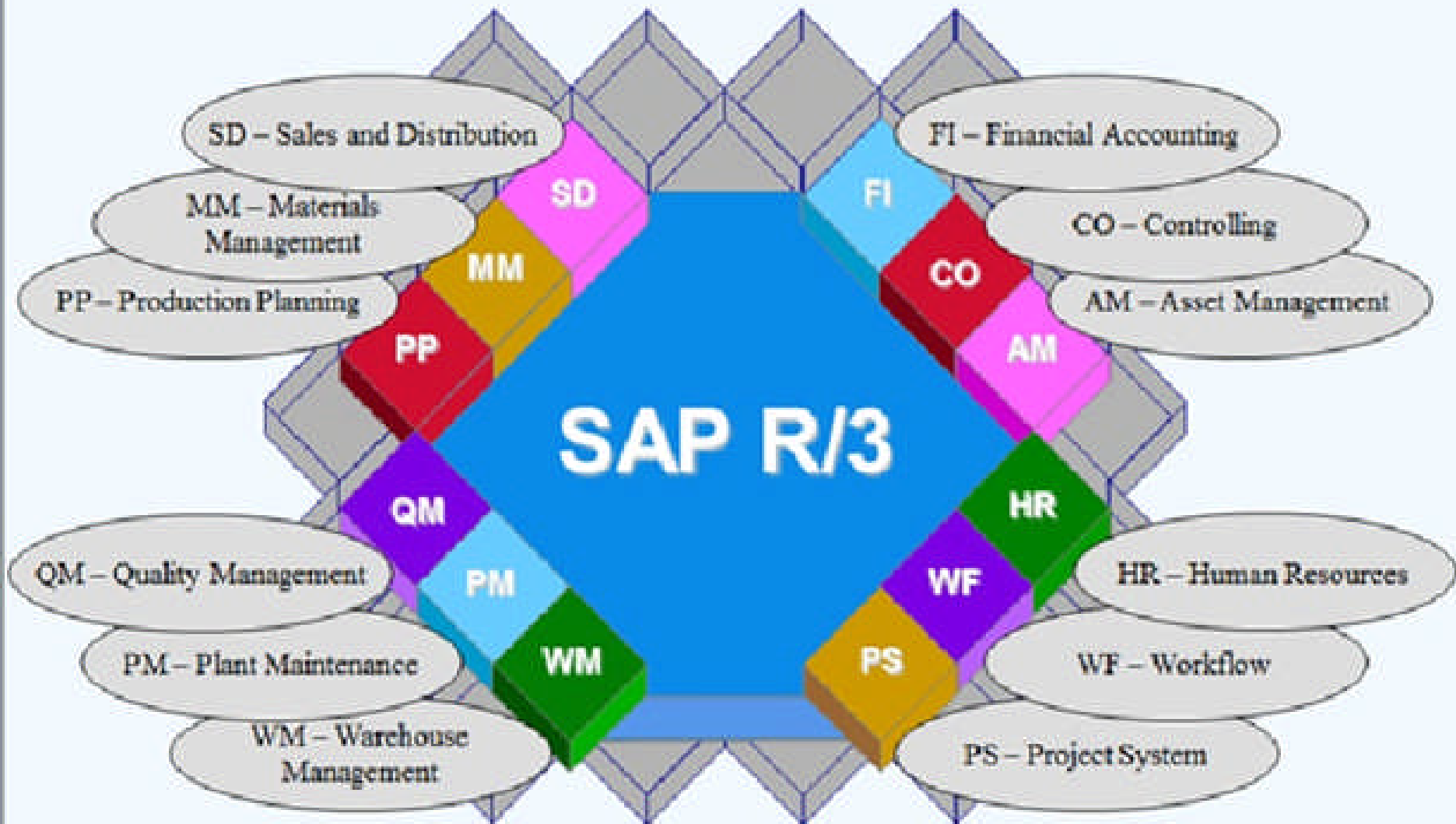
2.4 Correction and Transport System



•Moving changes from one R/3 system to another



SAP Modules



•2.5 SAP R/3 Modules [... contd.]

➤ SAP-FI (FInancial Accounting)

- SAP FI - General Ledger (GL)
- SAP FI - Accounts Payable (AP)
- SAP FI - Account Receivable (AR)
- SAP FI - Bank Accounting

➤ SAP-SD (Sales & Distribution)

- SAP SD - Master Data
- SAP SD - Sales
- SAP SD - Shipping
- SAP SD - Transportation
- SAP SD - Billing
- SAP SD - Electronic Data Interchange (EDI)

➤ SAP-CO (COntrolling)

- SAP CO - Cost Element Accounting
- SAP CO - Cost Center Accounting
- SAP CO - Activity-Based Costing
- SAP CO - Product Cost Controlling
- SAP CO - Material Ledger

➤ SAP-MM (Material Management)

- SAP MM - Purchasing
- SAP MM - Inventory Management
- SAP MM - Warehouse Management
- SAP ML - Material Ledger

2.5 SAP R/3 Modules [... contd.]

➤ SAP-PP (Production Planning)

- SAP PP - Material Requirements Planning
- SAP PP - Capacity Requirement Planning
- SAP PP - Sales and Operations Planning
- SAP PP - Production orders
- SAP DS - Detailed Scheduling

➤ SAP-PS (Project System)

- SAP PS - Payments
- SAP PS - Confirmation
- SAP PS - Costs
- SAP PS - Resources
- SAP PS - Dates
- SAP PS - Documents

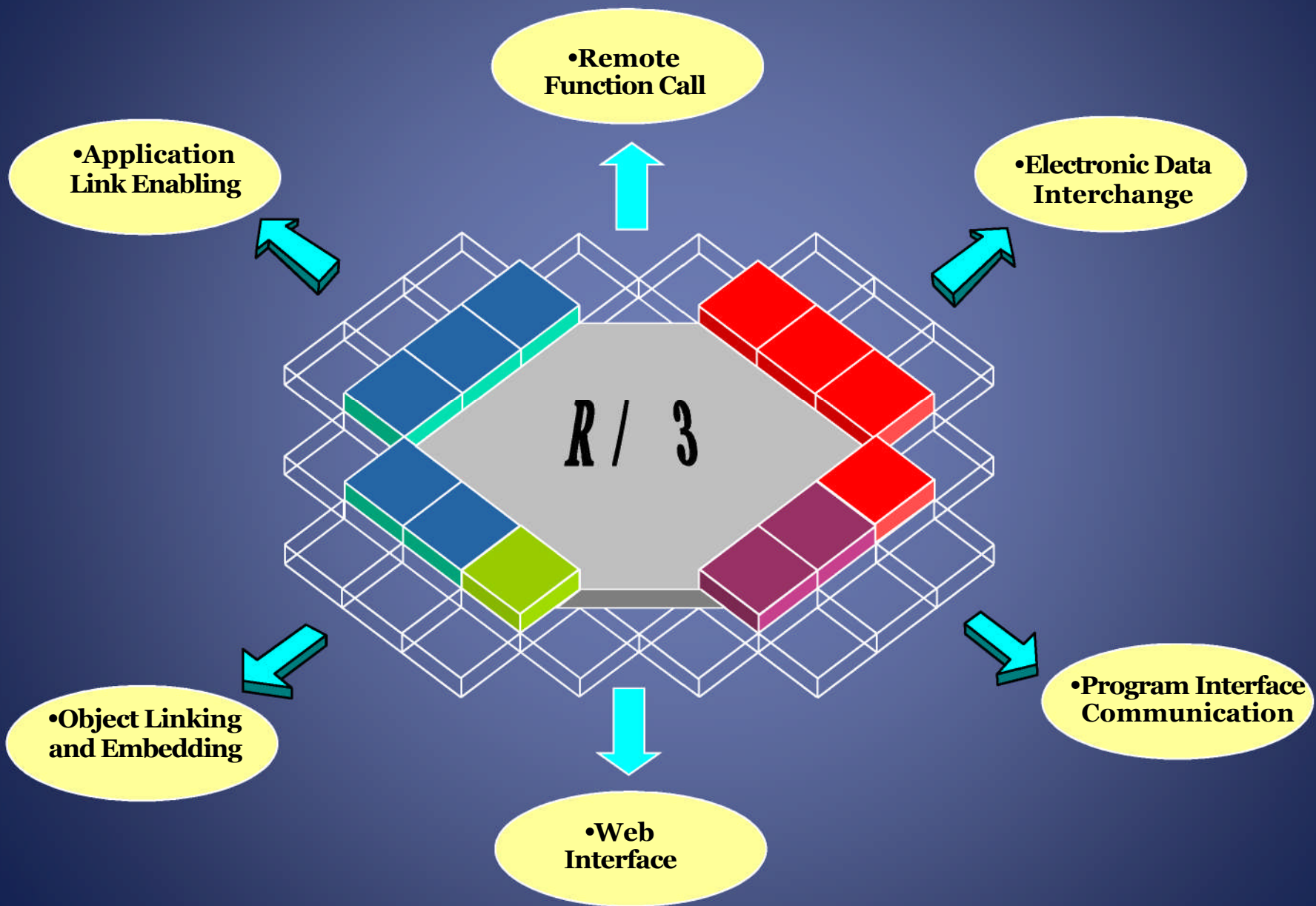
➤ SAP-HR (Human Resource)

- SAP PA - Employee Management
- SAP PA - Personnel Administration
- SAP PA - Benefits
- SAP PA - Payroll
- SAP PA - Time Management

➤ SAP-QM (Quality Management)

- SAP QM - Quality Planning
- SAP QM - Quality Inspection processing
- SAP QM - Quality control
- SAP QM - Test equipment management

2.6 R/3 Communication/Interfaces



2.7 SAP Product – features

- SAP R/3 Supports
 - Multiple Languages
 - Multiple Currencies
- Proprietary (High-level) Programming Language — ABAP (Advanced Business Application Programming)
- Can execute on any Operating System — UNIX,
 - Windows etc.
- Can use any Database — Oracle, MS SQL, MS
 - Access , SAP Hana
- Currently, no Support for versions other
 - than SAP R/3 ECC (ERP Central Component) 6.0

2.8 SAP – Points to Ponder

- Highly integrated
- On-line, Real-time
- Complex Data Structures
- Causes business process changes
- Causes organizational changes
- Very sophisticated testing of functionality
- and standard reports
- In-Built Controls -
 - Debit Credit tally
 - Trail of all transactions entered

2.9 SAP Business one

- SAP Business one — for Small / Medium Enterprises
- Not much complex as well as Not expensive as compared to SAP R/3
- Menu driven and **NOT** T-code (Transaction Code) driven as SAP R/3
- Not much customization is possible
- No modules needs to buy entire package and Restrictions can be done on the basis of License purchased
- Generally unable to rely on automated controls

SESSION 3

Accessing and Navigating SAP

3.1 Accessing SAP

- NEVER ACCESS LIVE ENVIRONMENT with INSERT/EDIT/DELETE RIGHTS
- Log-on only with "READ ONLY" Access

3.2 Logging On -SAP GUI

- To log on to an R/3 system with the SAP GUI, one need the proprietary SAP GUI (Graphical User Interface) software loaded on your system and an internet /network/VPN connection



- Account on
- SAP R/3 System
- at Data Centre or hosting site

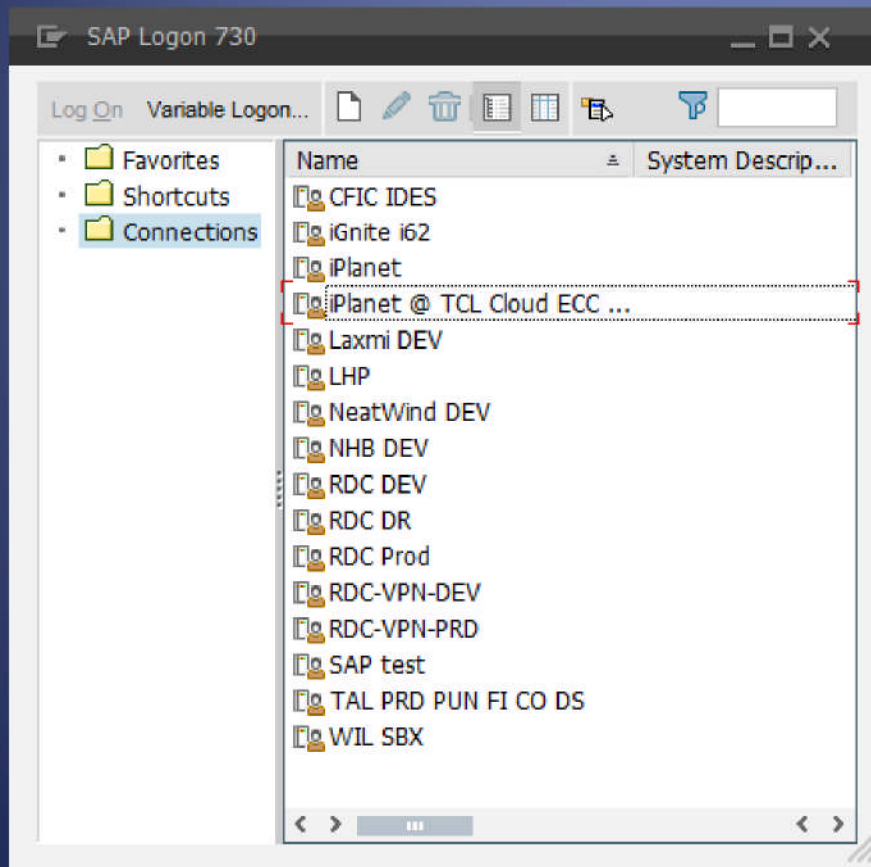
- Internet / Network, VPN
- Connection



- PC with SAP GUI

3.3 SAP GUI Configuration

- First, you need to tell the SAP GUI which system you want to log into:



3.4 System Definition

System Entry Properties

Connection Network Code Page

Choose the connection type and change the system parameters as required. Delete the old description if you want the system to propose a description. Button 'OK' is only active when all required input data has been entered.

Connection Type: Custom Application Server

System Connection Parameters

Description: iPlanet @ TCL Cloud ECC 007 EHP6

Application Server: [REDACTED]

Instance Number: 00

System ID: EH6

SAProuter String: [REDACTED]

OK Cancel Help

•Text description (free)

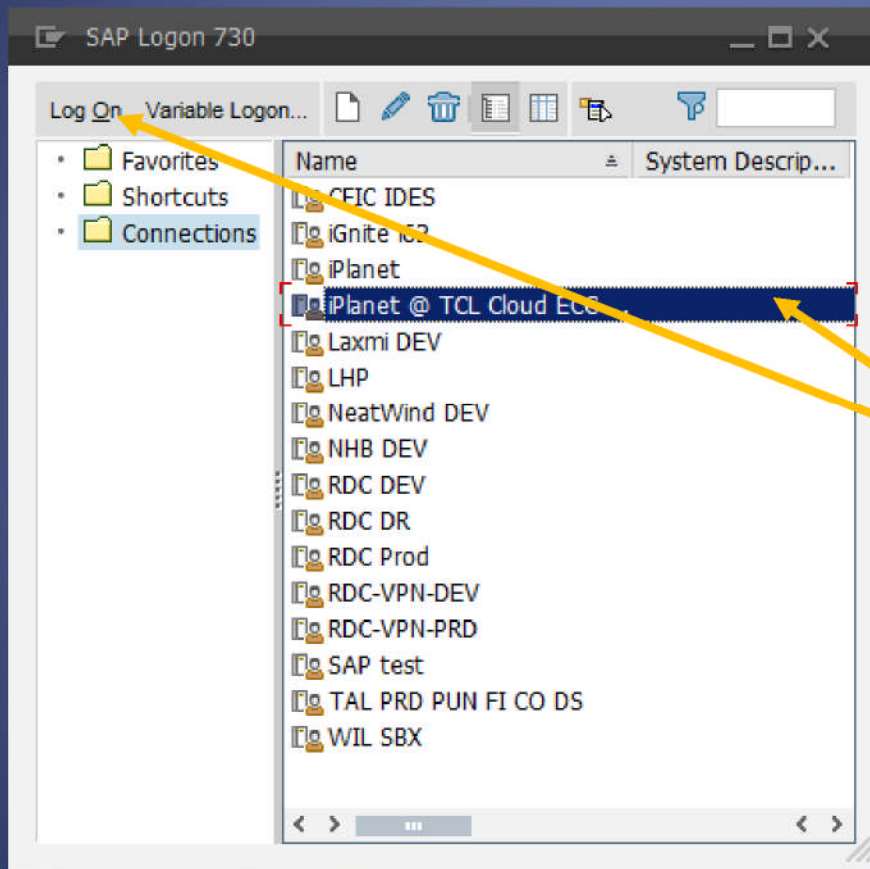
•Address of system (e.g. sapd.umssystem.edu)

•System Number

•System ID
•Logical name of system

•SAP Router (usually not required)

3.5 Configured SAP GUI



- Select System:
- double-click or
- Logon button

3.6 Logging On

The screenshot shows the SAP login interface. At the top, there is a menu bar with 'User', 'System', and 'Help'. Below the menu bar is a toolbar with a green checkmark, a dropdown arrow, and several navigation icons. The main area is titled 'SAP' and contains a 'New password' section. Below this, there are four input fields: 'Client' with the value '500', 'User' (empty), 'Password' (masked with asterisks), and 'Language' (empty). Yellow arrows point from the text annotations on the right to each of these four input fields.

•Enter Client

•Enter User (R/3 Account)

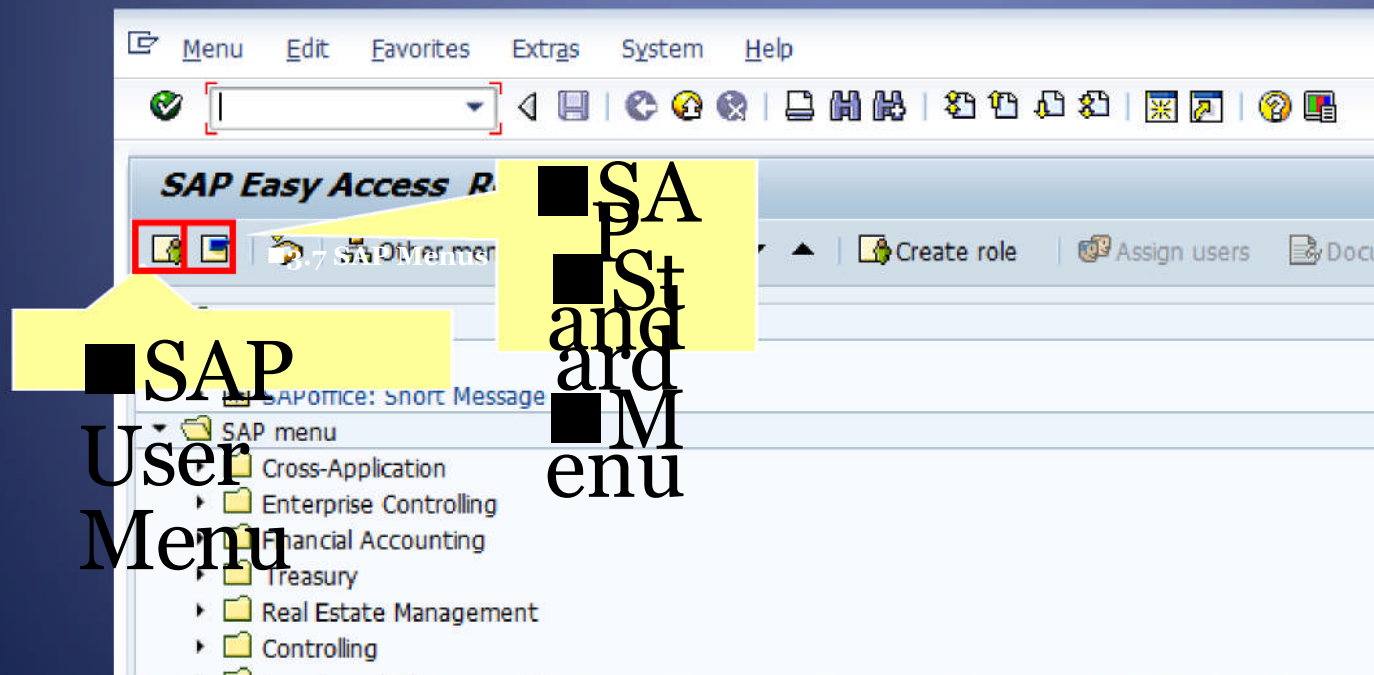
•Enter Password (R/3 Account)

•Don't worry about language—

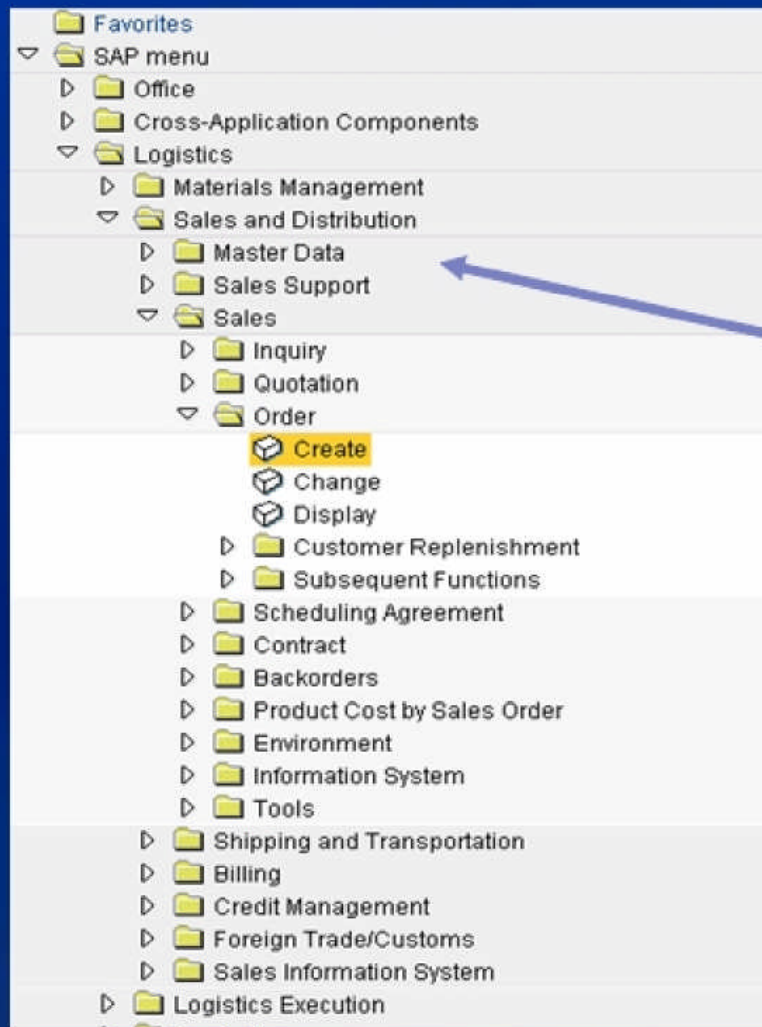
•English will default in

3.7 SAP Menus

- The default screen is called the *SAP Easy Access* Screen.
 - You can switch from one menu to the other by selecting the appropriate icon
 - When you log on, you will see either your user menu (specific to your role), or the SAP standard menu (lists all transactions)



3.8 SAP Navigation: Using the System



• Two ways to choose a task:

• Clicking on the menu option

• Enter a transaction code in the command field

3.9 SAP Screen Components

The screenshot shows the SAP Easy Access interface with several components highlighted by callouts:

- SAP Menu**: Points to the menu bar at the top.
- Buttons**: Points to the toolbar below the menu bar.
- Favorites**: Points to the left-hand navigation tree.
- Title Bar**: Points to the top window title bar.
- Standard Toolbar**: Points to the toolbar below the title bar.
- Navigation icons**: Points to the icons in the toolbar.
- Application Toolbar**: Points to the toolbar below the navigation icons.
- Command Field**: Points to the input field in the toolbar.
- Message Bar**: Points to the bar at the bottom of the screen.
- Status Bar**: Points to the bottom status bar.

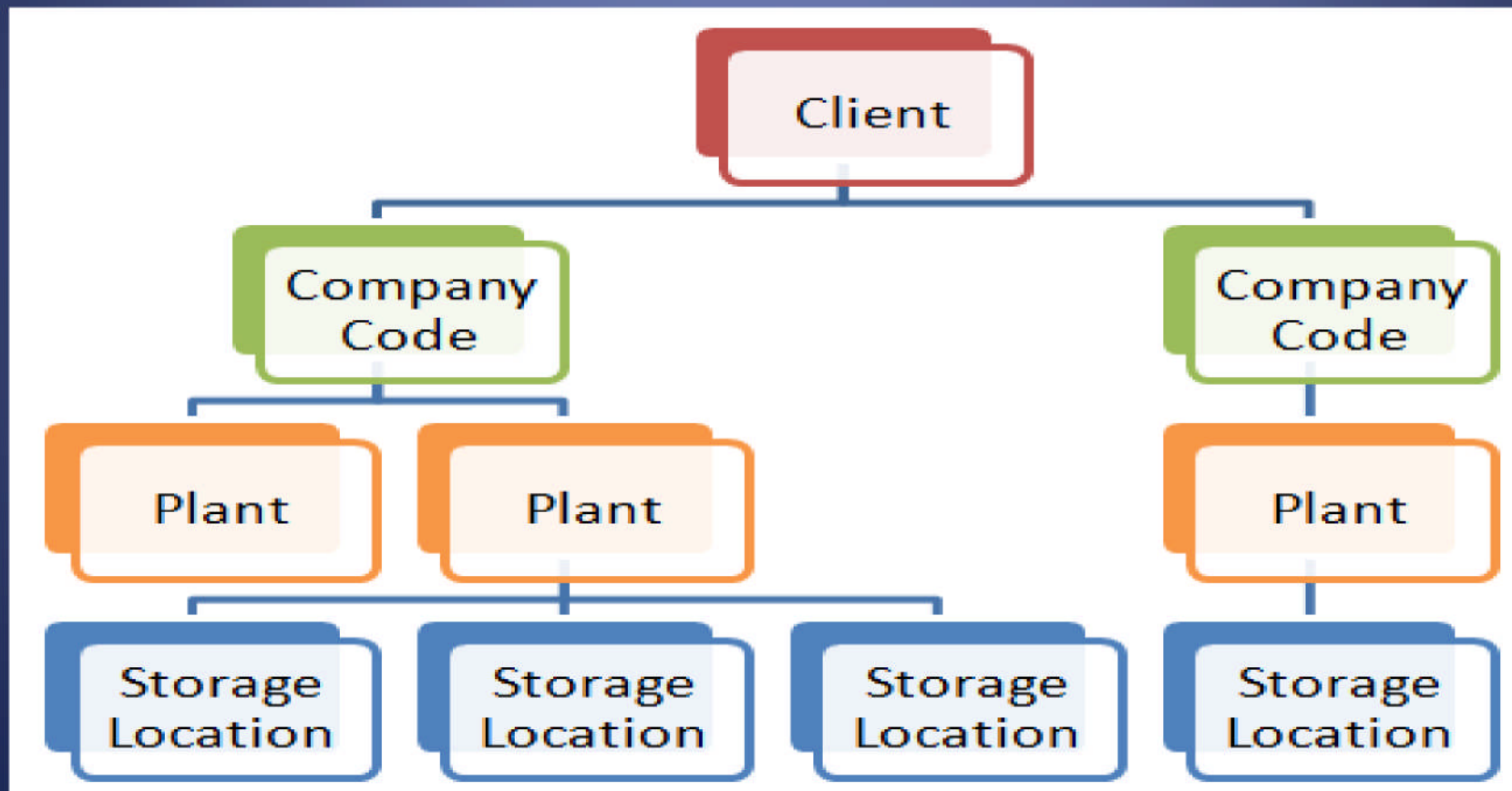
•Caution:

- Depending on your GUI version,
- the screen may
- look different
- even if the SAP
- version is the
- same!

SESSION 4

SAP Organization

4.1 SAP R/3 Organization Structure



4.2 SAP Organization

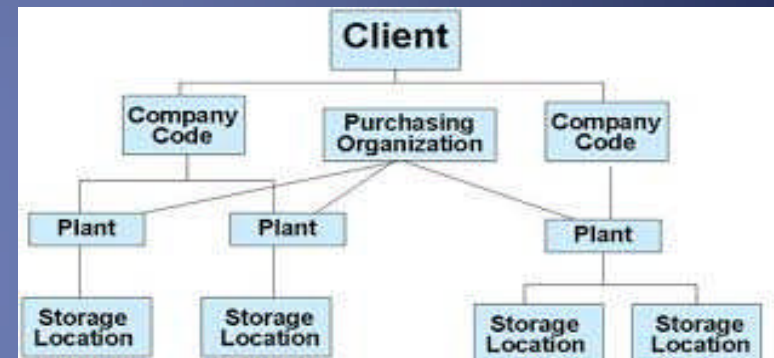
- Instance — One installation
- Client — At least one Client per Instance
- Company Code
 - At least one Company Code per Client
 - Generally a legal entity
 - Trial Balance can be drawn at this level
- Cross Instance settings are not possible
- Cross Client settings are possible
- Cross Client consolidations are possible
- Some data can be defined at Client level, will apply to all Company Codes of that Client

4.1 SAP OrganizationContd.

- Business Area — across Company Codes
- Plant — assigned to a single Company Code

- Purchasing Organization

- Sales Organization



- Very difficult to change SAP Organization after implementation
- Definition is extremely important for functionalities and security

4.2 SAP Organization Impact on Audit

- Appropriate scoping
- New GL for Multiple Reporting(s) — IFRS, Foreign Reporting, Statutory and Tax Reporting
- Consolidations

SESSION 5

Review of IT General Controls (Other than BASIS)

5.0 IT General Controls

ITGCs may also be referred to as General Computer Controls which are defined as

"Controls, other than application controls which, relate to the environment within which computer-based application systems are developed, maintained and operated and which are therefore applicable to all applications"

5.0 IT General Controls

- ITGCs cover 5 domains -
 - IT Governance
 - Access to Programs and Data
 - Change Management
 - Program Development
 - Computer Operations
- The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations.
- Like application controls, general controls may be either manual or programmed.

5.1 IT Governance

- Management controls over IT
- IT Organization structure, including definition of roles and responsibilities within IT
- Policies and Procedures, e.g.
 - IT Security Policies
 - Change Management
 - Infrastructure maintenance
 - HR Policies
- Regulatory compliance
- Audit issues management

5.2 Access to Programs and Data

- Provisioning and modification of end-user access (SAP, Operating Systems, Databases, Networks)
- Timely revocation of user access (resigned/absconded users)
- Privileged access to SAP, Operating Systems, Databases, Networks
- Physical Accesses (access to data center, computing facilities, environmental controls)
- Password parameters

5.2 IT Risks within Access to Programs and Data

- User access is provided without appropriate prior approvals
- User access for terminated employees is not removed in a timely manner
- User access is appropriately updated to reflect changes to individuals roles and responsibilities
- Access to the system is restricted through complex password parameters

5.2 Auditing in SAP

- Verify that access to critical system (application, operating system and database) functions is appropriately restricted on an as-needed basis
- Super-user profiles, i.e. SAP_ALL and SAP_NEW are not assigned to any user id
- Default SAP Accounts are locked and their default passwords are changed
- Privileged (super-user) user access at the application, OS, database and network level is approved
- Complex passwords are required at all levels

5.2 Auditing in SAP

- Logging is enabled at the system level and critical configuration tables are logged
- Remote access (VPN, Web, etc.) is appropriately restricted and monitored
- User accounts that support internal processes, interfaces, job schedules, etc. are defined as system accounts (user types 'B' or 'C') to prevent individuals from using those accounts

5.2 Auditing in SAP

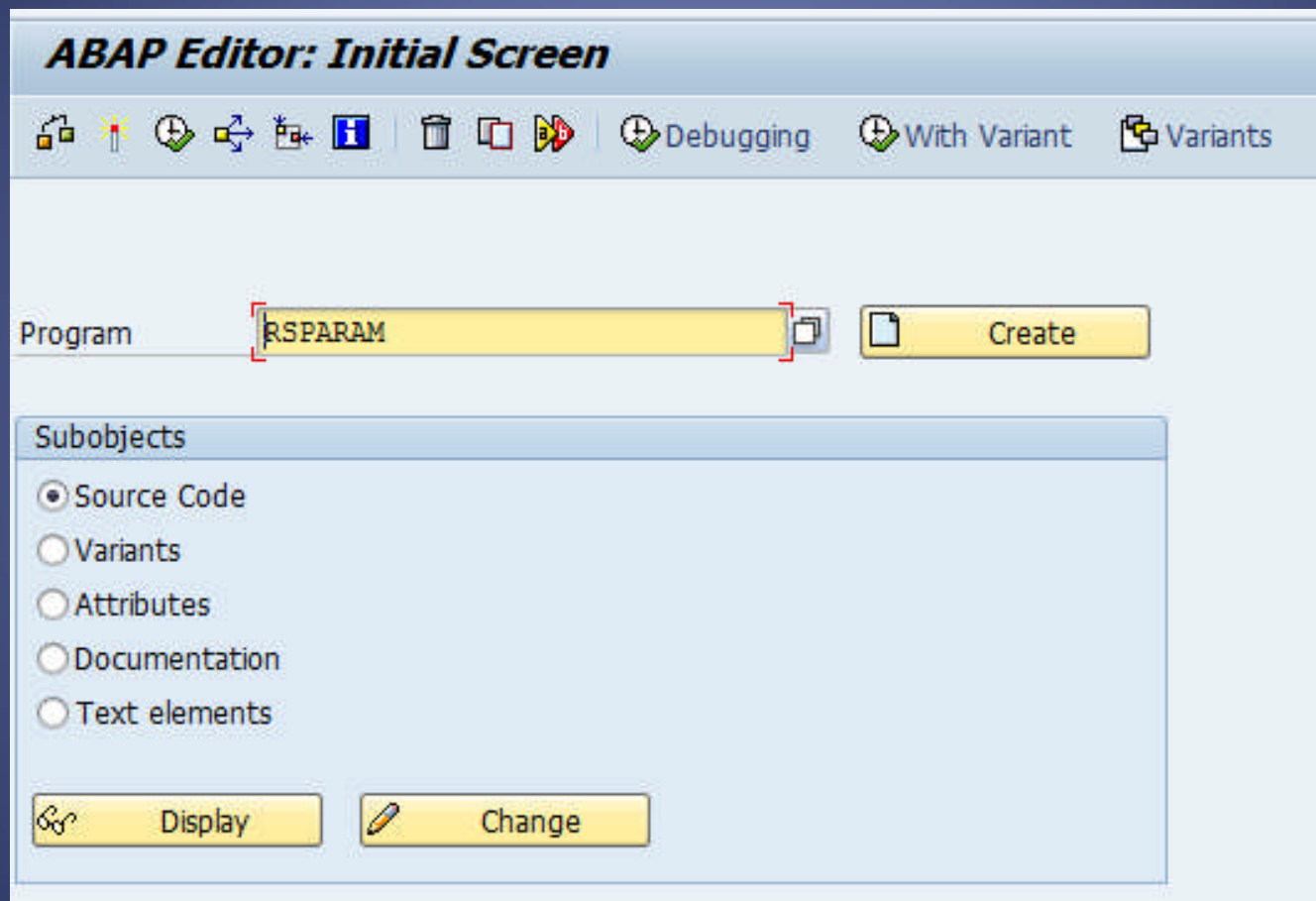
Data Browser: Table USR02 Select Entries 500

Check Table...

Table: USR02
Displayed Fields: 7 of 7 Fixed Columns: [2] List Width 0250

	User	Valid from	Valid through	User Type	User Lock	Created On	Last Logon Date
<input type="checkbox"/>	BITRAGNA	00.00.0000	00.00.0000	A	0	10.12.2013	00.00.0000
<input type="checkbox"/>	CAMPSTME	00.00.0000	00.00.0000	A	0	30.07.2013	00.00.0000
<input type="checkbox"/>	GARRISLA	00.00.0000	00.00.0000	A	32	23.09.2009	23.09.2009
<input type="checkbox"/>	02573A7B3F1	18.05.2006	31.12.9999	A	0	18.05.2006	18.05.2006
<input type="checkbox"/>	0434C129E41	31.03.2006	31.12.9999	A	0	31.03.2006	22.08.2006
<input type="checkbox"/>	04BFFB8C6607	01.01.1900	31.12.9999	S	0	11.03.2011	03.04.2014
<input type="checkbox"/>	04F9591D911	10.03.2008	31.12.9999	A	0	10.03.2008	10.03.2008
<input type="checkbox"/>	08741F8A221	30.06.2006	31.12.9999	A	0	30.06.2006	30.06.2006

5.2 Auditing in SAP



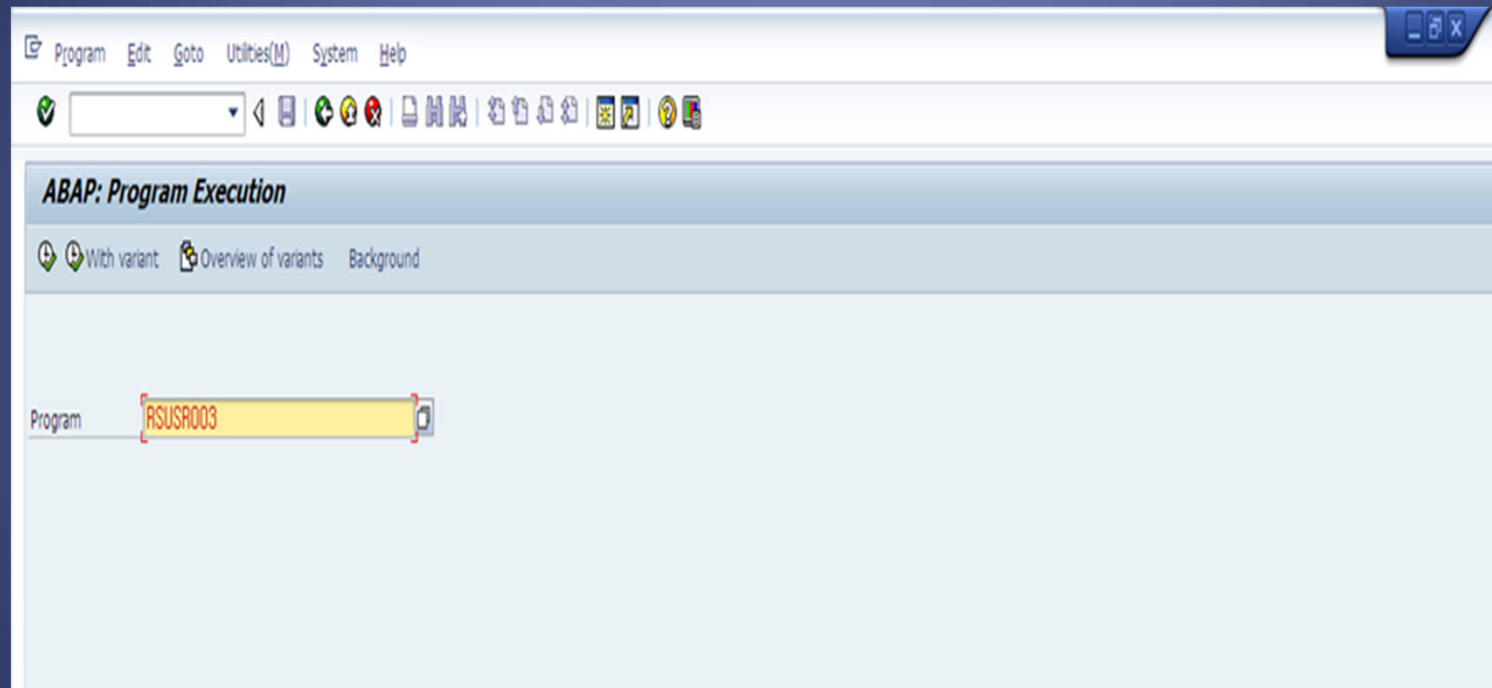
5.2 Auditing in SAP

Display Profile Parameter



Parameter Name	User-Defined Value	System Default Value	Parameter Name	Comment
login/min_password_digits		0		min. number of digits in passwords
login/min_password_lett...		0		min. number of letters in passwords
login/min_password_lng		6		Minimum Password Length
login/min_password_low...		0		minimum number of lower-case characters in passwords
login/min_password_spe...		0		min. number of special characters in passwords
login/min_password_upp...		0		minimum number of upper-case characters in passwords
login/multi_login_users				list of exceptional users: multiple logon allowed

5.2 Auditing in SAP



5.2 Auditing in SAP

Client	User	Lock	Password Status	Reason for User Lock
000	DDIC		Exists; Password not trivial.	
	SAP*		Does not exist. Logon not possible. See SAP Note 2383	
	SAPCPIC		Password ADMIN well known. See SAP Note 29276	
	TMSADM		Password PASSWORD is well known	
001	DDIC		Exists; Password not trivial.	Locked by administrator
	SAP*		Exists; Password not trivial.	
	SAPCPIC		Password ADMIN well known. See SAP Note 29276	
	TMSADM		Does not exist.	
066	DDIC		Does not exist.	
	EARLYWATCH		Password SUPPORT well known.	
	SAP*		Password 06071992 well known.	
	SAPCPIC		Does not exist.	
	TMSADM		Does not exist.	
301	DDIC		Exists; Password not trivial.	
	SAP*		Does not exist. Logon not possible. See SAP Note 2383	
	SAPCPIC		Does not exist.	
	TMSADM		Does not exist.	

5.3 Change Management

- Changes to application configurations, reports, programs
- Changes to Operating Systems, databases and network
- Segregation of environments (development, test and production)
- Developer Access to live data is restricted

5.3 IT Risks within Change Management

- Unauthorized changes are made to the application, operating system, database or network
- Changes are not tested sufficiently prior to implementation in the production system

5.3 Auditing in SAP

- SAP environment is segregated into the 3-box system, i.e. development, testing/QA and production (live)
- Changes are adequately and independently tested and approved before being implemented in the production
- Developers should not have access to production either through developer keys or through transactions.
- Production is locked for direct changes and is opened based on specific approvals
- When direct changes are required in production, they are made only through transport requests
- Business impact analysis of changes implemented

5.3 Auditing in SAP

Data Browser: Initial Screen






   

Table Name 

5.3 Auditing in SAP

Data Browser: Table E070 Select Entries 500





Check Table...

Table: E070
Displayed Fields: 8 of 8 Fixed Columns: [1] List Width 0250

Request/Task	Status	Transport Target	Category	Owner	Date	Time	Short Description
<input type="checkbox"/> DE3K904146	R	CL5	SYST	CHANDRAS	05.05.2006	16:08:08	HR Topline
<input type="checkbox"/> DE3K904139	R	CL5	SYST	SHAHA	05.05.2006	15:43:25	Changes to ZPYXXFO_ZSAP_PAYSLIP_US2 form
<input type="checkbox"/> DE3K904116	R	CL5	SYST	PITTEN	05.05.2006	23:22:34	Fix MSS budget
<input type="checkbox"/> DE3K904068	R	CL5	SYST	SOHN	11.05.2006	20:19:53	ERecruiting Succession for Beth Solomon
<input type="checkbox"/> DE3K904049	R	CL5	CUST	C5073548	29.05.2006	21:26:51	Ticket 85133
<input type="checkbox"/> DE3K904029	R	CL5	SYST	CHANDRAS	28.04.2006	19:14:51	HR Topline
<input type="checkbox"/> DE3K903983	R	CL5	SYST	SOLOMON	27.04.2006	19:35:50	Workbench changes for e-recruiting-BES

5.3 Auditing in SAP

Display View "Clients": Details

Client	<input type="text" value="001"/> IDES Sandbox		
City	<input type="text" value="MUNICH"/>	Last Changed By	<input type="text" value="CATT_USER"/>
Logical system	<input type="text" value="E6ICLNT801"/>	Date	<input type="text" value="16.04.2014"/>
Std currency	<input type="text" value="EUR"/>		
Client role	<input type="text" value="Demo"/>		


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

5.3 Auditing in SAP

Change Documents for Users





Standard Selection

User	<input type="text"/>	to	<input type="text"/>
Changes by	<input type="text"/>	to	<input type="text"/>
From Date	01.04.2015		Week
From Time	00:00:00		
To Date	30.06.2015 		
To Time	23:59:59		

Output

- List of the Change History
- Table of Status History (User Attributes Horizontal)
- List of Status History (User Attributes Vertical)
- Technical View

Selection Criteria for Changed Authorizations

- Added Profiles
Profile Name: to
- Deleted Profiles
Profile Name: to
- Created Users
- Deleted Users

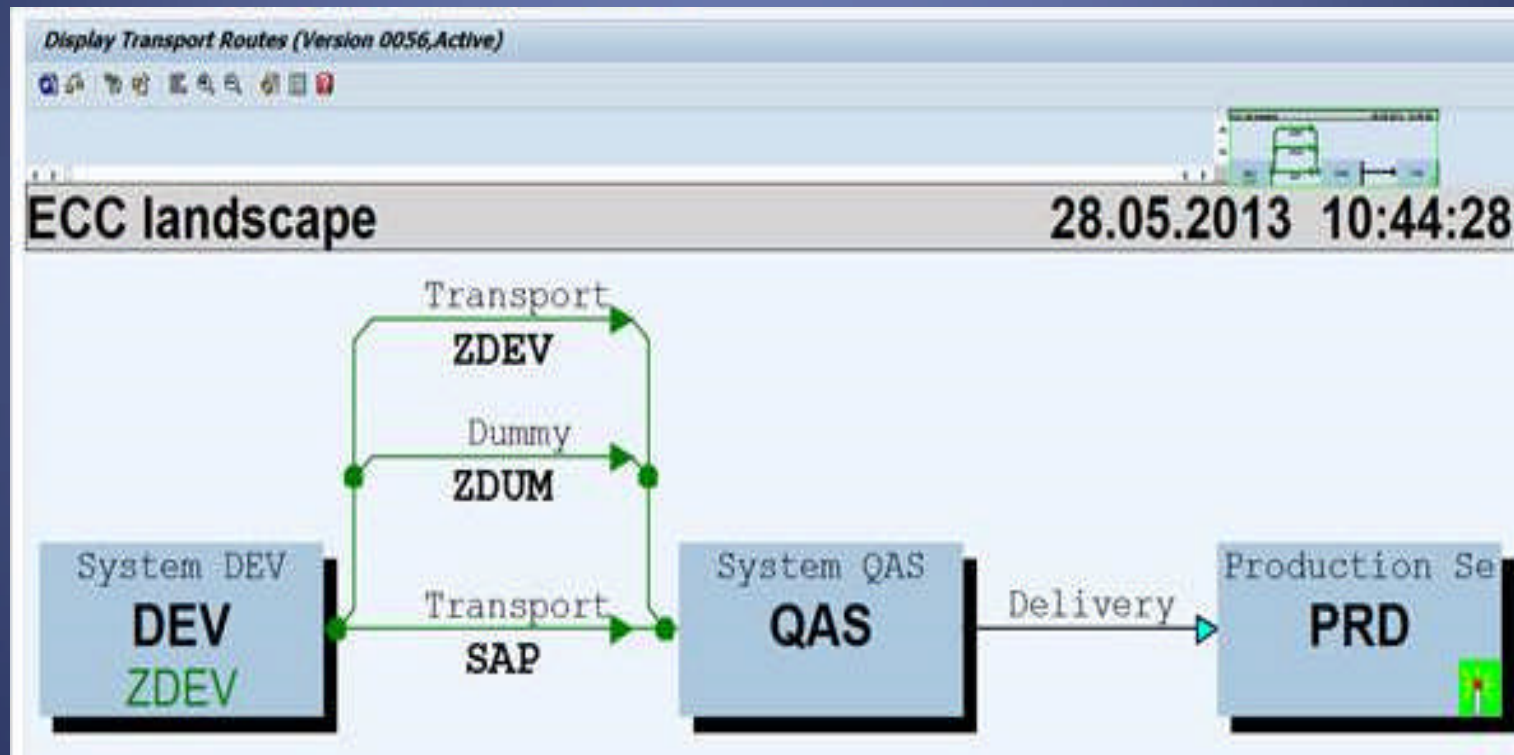
5.3 Auditing in SAP

Change Documents for Users

Number of Selected Change Documents: 1.617

User Na...	Date	Time	Changed by	Action	Old Value	Text for Value	New Value	Text for the New Value
ABRAHAGE	31.05.2015	23:34:49	MOLLETKI	Lock Changed	128	Incorrect Log...	0	Not locked
		23:35:06	MOLLETKI	Password Changed	Long Passw...		Long Password 2	
			MOLLETKI	Password status changed	Productive		Initial	
ABRAMEYA	12.04.2015	11:35:22	ABRAMEYA	Password Changed	Long Passw...		Long Password 2	
			ABRAMEYA	Password status changed	Initial		Productive	
AMANGU	10.04.2015	07:06:10	AMANGU	Password Changed	Long Passw...		Long Password 2	
			AMANGU	Password status changed	Initial		Productive	
AMULYARA	09.04.2015	18:52:51	MOLLETKI	User created				
			MOLLETKI	Initial User Type			A	Dialog User
			MOLLETKI	Password Changed			Long Password 1	
			MOLLETKI	Password status changed			Initial	
			MOLLETKI	Profile Added			T-EI0100293	Profile for role Z:R3_PROJECT_...
			MOLLETKI	Profile Added			T-EI0100292	Profile for role Z:R3_PROJECT_...
			MOLLETKI	Profile Added			T-EI0100291	Profile for role Z:R3_PROJECT_...
			MOLLETKI	Profile Added			T-EI010029	Profile for role Z:R3_PROJECT_...

5.3 Auditing in SAP



5.4 Computer Operations

- Batch Processing and scheduling
- Interface testing
- Backup
- Disaster Recovery and BCP
- Network security

5.4 IT Risks within Computer Operations

- Failed batch jobs are not monitored and rescheduled
- Interfaces are not monitored
- System back-ups are not taken on a regular basis
- Back-ups are not tested for successful restoration
- Back-ups are not stored at an offsite location
- External access to the system is not appropriately restricted
- Data center is not designed to prevent damage due to heating, accidental fires, etc.

5.4 Auditing in SAP

- Access to batch scheduling and monitoring tools is restricted to the IT operations team
- Access to back-up tools is restricted to the IT operations team
- Failed batch jobs, interfaces and back-ups are tracked through a ticketing system and are resolved
- Back-ups are stored at an offsite location and are periodically tested for successful restoration
- External access to the system is appropriately restricted through firewalls, etc. and periodically tested

SESSION 6

Review of SAP BASIS

6.0 SAP Basis review

ITGC Domain – Computer Operations

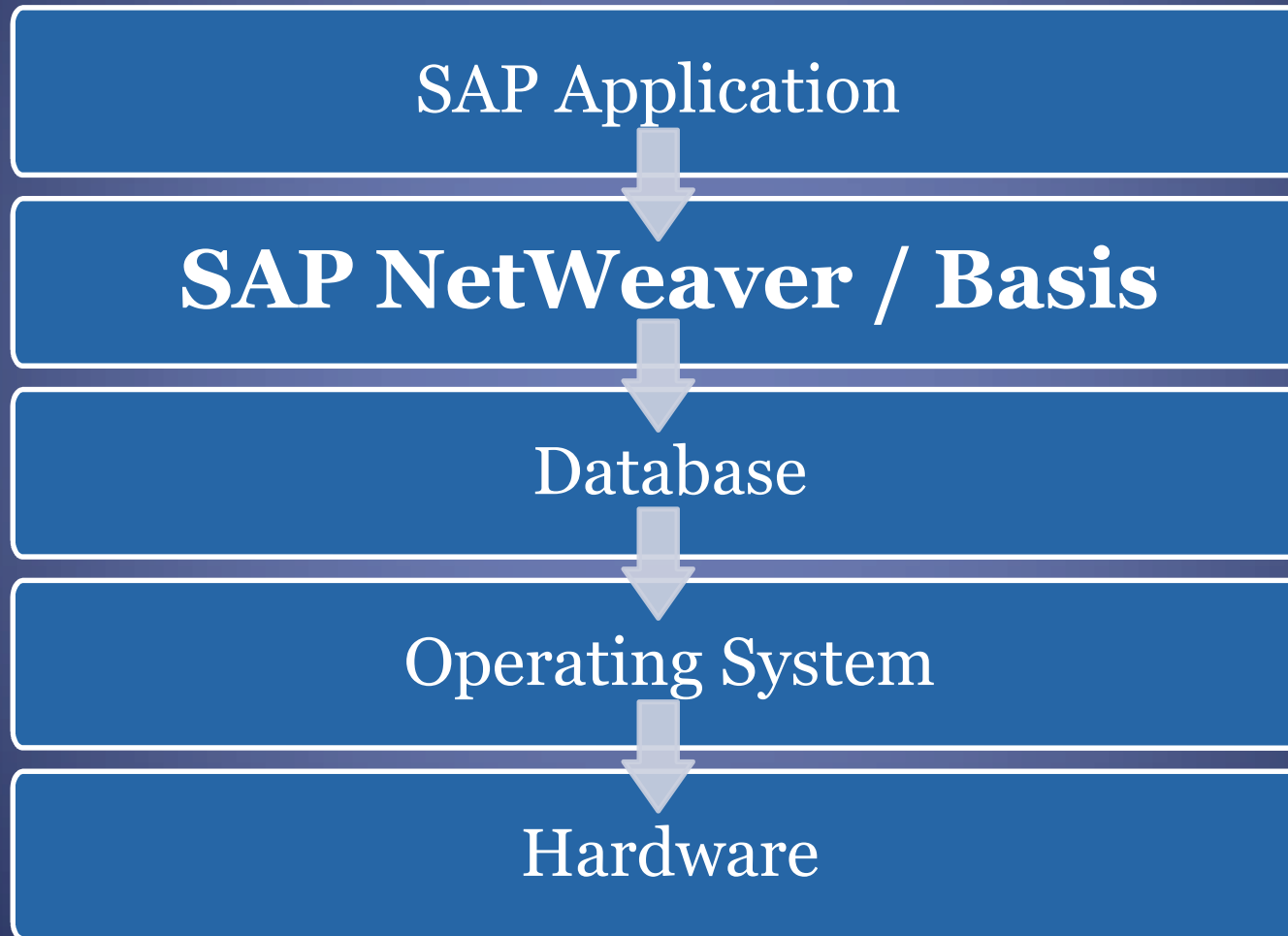
- Access to maintain (create new or change/delete existing) job schedules is appropriately restricted
- Access to executed critical job schedules is appropriately restricted
- Critical batch jobs, especially those that have a financial impact, are identified and are monitored
- Failed batches are monitored and resolved

The above procedures apply like-wise to any interfaces that have been set-up with external applications

6.0 SAP NetWeaver / Basis

- What is SAP NetWeaver / Basis
- Role of SAP Basis team member
- IT Risks within SAP Basis
- SAP Basis review

6.1 What is SAP NetWeaver / Basis?



6.1 What is SAP NetWeaver / Basis?

- NetWeaver is a toolkit used to enhance business functionalities delivered by SAP components.
- Often interchangeably referred to as **SAP Basis** (reference to the original toolkit that was the foundation of SAP R/3).
- Act as a filter between the actual business logic in SAP R/3 and the specifics of the operating system and database underneath.
- SAP business programmers could focus on writing business logic and not have to worry whether or not it would work on the various permutations of hardware, operating system and/or database.

6.2 Role of SAP Basis team member

- Activities that an SAP NetWeaver System Administrator does day-to-day, include:
 - create users/assign roles (within SAP)
 - run backup
 - check db/os space utilization, add space if necessary
 - install SAP software, configure SAP parameters
 - monitor CPU/Memory/disk space/performance
 - configure connectivity between SAP components or SAP/non-SAP components
 - SAP software change management (i.e. Transport Management).

6.3 IT Risks within SAP Basis

- Critical system administration access is not appropriately restricted, e.g.
 - super-user access across the application
 - creating/modifying user access and roles
 - direct access to data through table maintenance
 - opening production (live) system for making direct changes
 - applying tested and approved changes to the production system
 - access execute programs directly in production system
 - access to execute operating system and database commands
 - access to application activity logs
 - access to manage interfaces with other applications
 - access to modify system parameters (passwords, logging, etc.)

6.3 IT Risks within SAP Basis

- Conflicting accesses not appropriately segregated, e.g.
 - access develop/code a change AND implement it in the production system
 - developers have access to production environment
- Activities performed by Basis team members are not logged and reviewed periodically, e.g.
 - review of security audit logs for critical activities
 - where change transports are owned and implemented by Basis team, they are adequately and independently tested prior to implementation

SESSION 7

Validation of Automated Controls

7. Business Cycles

- General Ledger
- Sales – Receivables
- Purchase – Payables
- Inventory
- Fixed Assets
- Payroll

7.1 General Ledger Cycle

- GL accounting master data –
 - At Chart of Accounts level
 - At Company code level
- GL “Autopost” Configuration
- GL – Sub ledger linking through “Recon” accounts
- Period closures – FI/MM
- 12+4 periods

- Reconciliation Account Type

G/L Account 15444 test
Company Code 1000 Subsidiary Germany

Account control in company code

Account currency EUR Euro (EMU currency as of 01/01/1999)

Only balances in local crcy

Exchange rate difference key

Valuation group

Tax category

Posting without tax allowed

Recon. account for acct type

- Auto Post Indicator

G/L Account 15444 test
Company Code 1000 Subsidiary Germany

Control of document creation in company code

Field status group 6001 General (with text, allocation)

Post automatically only

Supplement auto. postings

7.2 Sales - Receivables Cycle

- Master Data –
 - Customer Master
 - Material Master
 - Price Master
 - Credit Management for customer
- Access to Master Data
- Monitoring modifications to Master Data

7.2 Sales - Receivables Cycle – contd..

- Sales Account Determination

Cust.Grp/MaterialGrp/AcctKey									
App	CndTy.	ChAc	SOrg.	AAG	AAG	ActKy	G/L Account	Provision acc.	
V	KOFI	MFG	1010	DO	AS	ERL	6410003		
V	KOFI	MFG	1010	DO	R3	ERL	6000055		

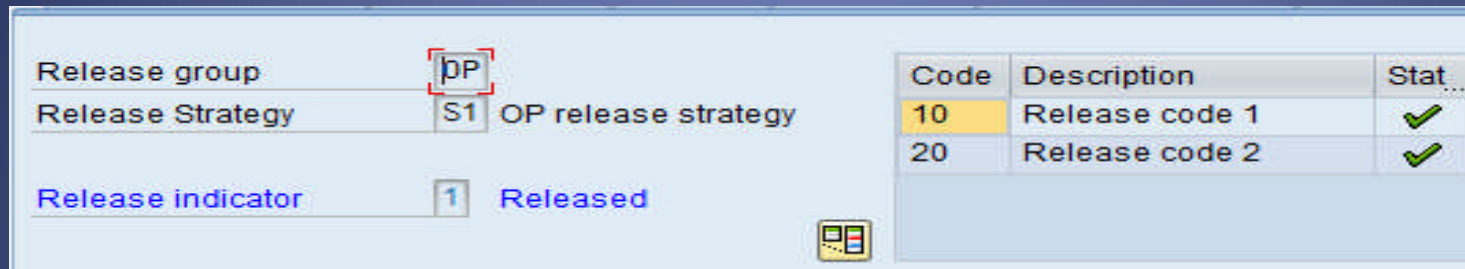
- Ageing of Debtors – settings for “Payment Terms from Invoice”

Specifications for Posting Residual Items from Payment Differences	
<input checked="" type="checkbox"/> Payment Term from Invoice	Fixed payment term <input type="text"/>

- Manual Entries to Sales-related accounts
- Sales order – Delivery – Invoice linking

7.3 Purchase - Payables Cycle

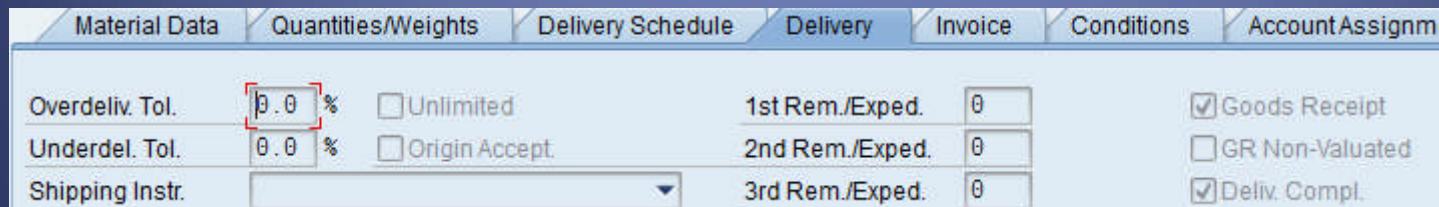
- Purchase Order Approval



The screenshot shows the SAP Purchase Order Release Strategy configuration. The 'Release group' is set to 'OP' (highlighted with a red box). The 'Release Strategy' is 'S1' with the description 'OP release strategy'. The 'Release indicator' is '1' with the label 'Released'. A table on the right lists release codes:

Code	Description	Stat...
10	Release code 1	✓
20	Release code 2	✓

- 3 way match configuration (PO – GR - IR)



The screenshot shows the SAP 3-way match configuration. The 'Overdeliv. Tol.' is set to '0.0' % (highlighted with a red box). The 'Underdel. Tol.' is also set to '0.0' %. The 'Shipping Instr.' is set to a dropdown menu. The '1st Rem./Exped.', '2nd Rem./Exped.', and '3rd Rem./Exped.' are all set to '0'. The 'Goods Receipt' and 'Deliv. Compl.' checkboxes are checked.

Material Data	Quantities/Weights	Delivery Schedule	Delivery	Invoice	Conditions	Account Assignm
Overdeliv. Tol.	0.0 %	<input type="checkbox"/> Unlimited	1st Rem./Exped.	0	<input checked="" type="checkbox"/> Goods Receipt	
Underdel. Tol.	0.0 %	<input type="checkbox"/> Origin Accept.	2nd Rem./Exped.	0	<input type="checkbox"/> GR Non-Valuated	
Shipping Instr.			3rd Rem./Exped.	0	<input checked="" type="checkbox"/> Deliv. Compl.	

- Unlimited Delivery whether only for scheduling agreement

7.3 Purchase - Payables Cycle – contd..

- Tolerances for Quantity and Price

Tolerance key	DQ	Exceed amount: quantity variance
Company Code	1000	Subsidiary Germany
Amounts in	EUR	Euro (EMU currency as of 01/01/1999)

Lower Limit	
Absolute	Percentage
<input type="radio"/> Do not check	<input type="radio"/> Do not check
<input checked="" type="radio"/> Check limit	<input checked="" type="radio"/> Check limit
Val. <input type="text" value="1.00"/>	Tolerance limit % <input type="text" value="2.00"/>

Upper Limit	
Absolute	Percentage
<input type="radio"/> Do not check	<input type="radio"/> Do not check
<input checked="" type="radio"/> Check limit	<input checked="" type="radio"/> Check limit
Val. <input type="text" value="3.00"/>	Tolerance limit % <input type="text" value="4.00"/>

7.3 Purchase - Payables Cycle – contd..

- Purchase Account Determination

Organization							
Plant	1000	>	Company Code	1000	->	Chart of Accounts	INT
			-> Valuation Area	1000	->	Valuation Grpg Code	0001
Valuation							
Material	R-B304				->	Valuation Class	7900
			Material Type	HALB	->	<input checked="" type="checkbox"/> Value Update	
Movement							
Movement Type	101		GR goods receipt				
Posting Lines							
Posting Lines Text	VIGCd	AGC	VC1	PK	Acct Deb.	PK	Acct Cr.
Gain/loss from revaluation	-e-	-e-	7900	83	232500	93	232500
Inventory posting	-e-	-e-	7900	89	790000	99	790000
Incidental costs of external a	-e-	-e-	-e-	86	415000	96	415000
External activity	-e-	-e-	7900	86	417002	96	417002
Change in stock account	-e-	-e-	7900	81	893010	91	893010
Purchase offsetting account	0001	-e-	7900	40	--Missing-	50	--Missing-
Purchase account	0001	-e-	7900	40	--Missing-	50	--Missing-
Materials management exch.rate	-e-	-e-	-e-	40	230000	50	280000
Cost (price) differences	-e-		7900	83	231500	93	281500
GR/IR clearing account	-e-	-e-	-e-	40	191100	50	191100
Inventory posting	-e-	-e-	7900	89	790000		

7.3 Purchase - Payables Cycle – contd..

- Vendor changeable in Invoice booking
- GR/IR Account for Goods
- Access to Master Data
- Payment processing –
 - Through direct cheques printing of due invoices
 - Through bank transfer via interface with bank portal (critical access)
- Ageing of Creditors – settings for “Payment Terms from Invoice”

7.4 Inventory Cycle

- Material master –
 - Price Control Indicator “V” / “S”
 - Costing Run
 - Bill of Material (BOM)

Valuation Class	7920
VC: Sales order stk	
Price control	S
Moving price	611.00
Total Stock	200

Current valuation	
Valuation Class	3000
VC: Sales order stk	
Price control	V
Moving price	11,773.96
Total Stock	169

Costing Structure	E.	Total v...	C...	L...	U	Resource	Plant
Bearing case	Δ	1,033.26 EUR	100 P...	1000	100-500		1000
• Ball bearing	■	920.00 EUR	100 P...	1000	100-510		

Cost Component View	Total Costs	Fixed	Variable	Currency
Cost of goods manufactur...	1,033.26	60.26	973.00	EUR
Cost of goods sold	1,410.70	99.60	1,311.10	EUR
Sales and administration ...	377.44	39.34	338.10	EUR
Inventory (commercial)	1,033.26	60.26	973.00	EUR
Inventory (tax-based)	1,033.26	60.26	973.00	EUR

Priority	Strategy Sequence	Incl. Additive Costs
1	Valuation Price According to Price Control in Ma...	<input checked="" type="checkbox"/>
2	Standard Price	<input checked="" type="checkbox"/>
3	Current Planned Price	<input checked="" type="checkbox"/>
4	Moving Average Price	<input checked="" type="checkbox"/>
5		<input type="checkbox"/>

7.4 Inventory Cycle – contd..

- Valuation not necessarily per AS2
 - For Raw material
 - Valuation could be at Standard Cost
 - Comparison with NRV has to be carried out manually
 - For WIP/FG,
 - No scope to define Normal Capacity
 - No distinction between Fixed and Variable overheads
 - Excise Duty on Closing Stocks has to be valued separately
 - Comparison with NRV has to be carried out manually
- Access to Material master

7.4 Inventory Cycle – contd..

- Manual Entries to Inventory Account
- Manual Entries to Cost of Goods Sold Account
- Entries for Shortages/Excesses
- Critical – direct changes to material cost
- Negative stock
- Access to sensitive movement types –
501/309/261/701/711

7.5 Fixed Assets Cycle

- Asset Master Data

Asset 2306 0 Equipment 1
Class 2000 Machines decl. depr. Company Code 1000

General Time-dependent Allocations Origin Net Worth Tax Insurance Deprec. Areas

General data

Description Equipment 1

Asset main no. text Equipment 1

Acct determination 20000 Technical assets and machines

Asset 2306 Equipment 1
Class 2000 Machines decl. depr. Company Code 1000

General Time-dependent Allocations Origin Net Worth Tax Insurance Deprec. Areas

Valuation

Deact	A.	Depreciation area	DKey	UseLife	Prd	ODep Start	Index	Group
<input type="checkbox"/>	01	Book deprec.	LINS	10		012-01-2011		<input type="checkbox"/>
<input type="checkbox"/>	02	Book deprec.	LINS	10		012-01-2011		<input type="checkbox"/>
<input type="checkbox"/>	03	Book deprec.	LINS	10		012-01-2011		<input type="checkbox"/>
<input type="checkbox"/>	20	Cost-acc.	LINB	10		012-01-2011	00010	
<input type="checkbox"/>	60	Book deprec.	DG20	10		012-01-2011		<input type="checkbox"/>
<input type="checkbox"/>	61	Spec.tax dep	DG20	10		012-01-2011		<input type="checkbox"/>
<input type="checkbox"/>	63	Tax bal.sht.	DG20	10		012-01-2011		<input type="checkbox"/>

7.5 Fixed Assets Cycle

- Account determination

Chart of dep.	1000	NT chart of depreciation: India
Chart of Accts	NIT	coa for technologies
Account determ.	11000	Buildings
Deprec. area	1	Book depreciation

Acquisition account assignment		
Acquisition:Acquis. and production costs	21100000	Building
Acquisition: down payments	22600000	Down Payments
Contra account: Acquisition value		
Down-payments clearing account		
Acquisition from affiliated company		
Revenue frm post-capitaliz:		

- Depreciation Posting to GL

Chart of dep.	1000	NT chart of depreciation: India
---------------	------	---------------------------------

Ar.	Name of depreciation area	Real	G/L
1	Book depreciation	<input checked="" type="checkbox"/>	1
15	Depreciation as per Income Tax Act 1961	<input checked="" type="checkbox"/>	0
20	Cost-accounting depreciation	<input checked="" type="checkbox"/>	3
30	Consolidated balance sheet in local currency	<input checked="" type="checkbox"/>	0
31	Consolidated balance sheet in group currency	<input checked="" type="checkbox"/>	0
32	Book depreciation in group currency	<input checked="" type="checkbox"/>	0
41	Investment support deducted from asset	<input checked="" type="checkbox"/>	0
51	Investment support posted to liabilities	<input checked="" type="checkbox"/>	1

Posting in G/L	Short Descript.
0	Area Does Not Post
1	Area Posts in Realtime
2	Area Posts APC and Depreciation on Periodic Basis
3	Area Posts Depreciation Only
4	Area Posts APC Directly and Depreciation
5	Area Posts APC Only
6	Area Posts Only APC Directly

- Manual Entries to Depreciation Account

7.6 Payroll Cycle

- Access to Masters
- Payroll Schemas
- Payroll Run
- Account Determination
- Manual Entries to Payroll Accounts

SESSION 8

Authorization Concept

8.1 Users and Authorizations

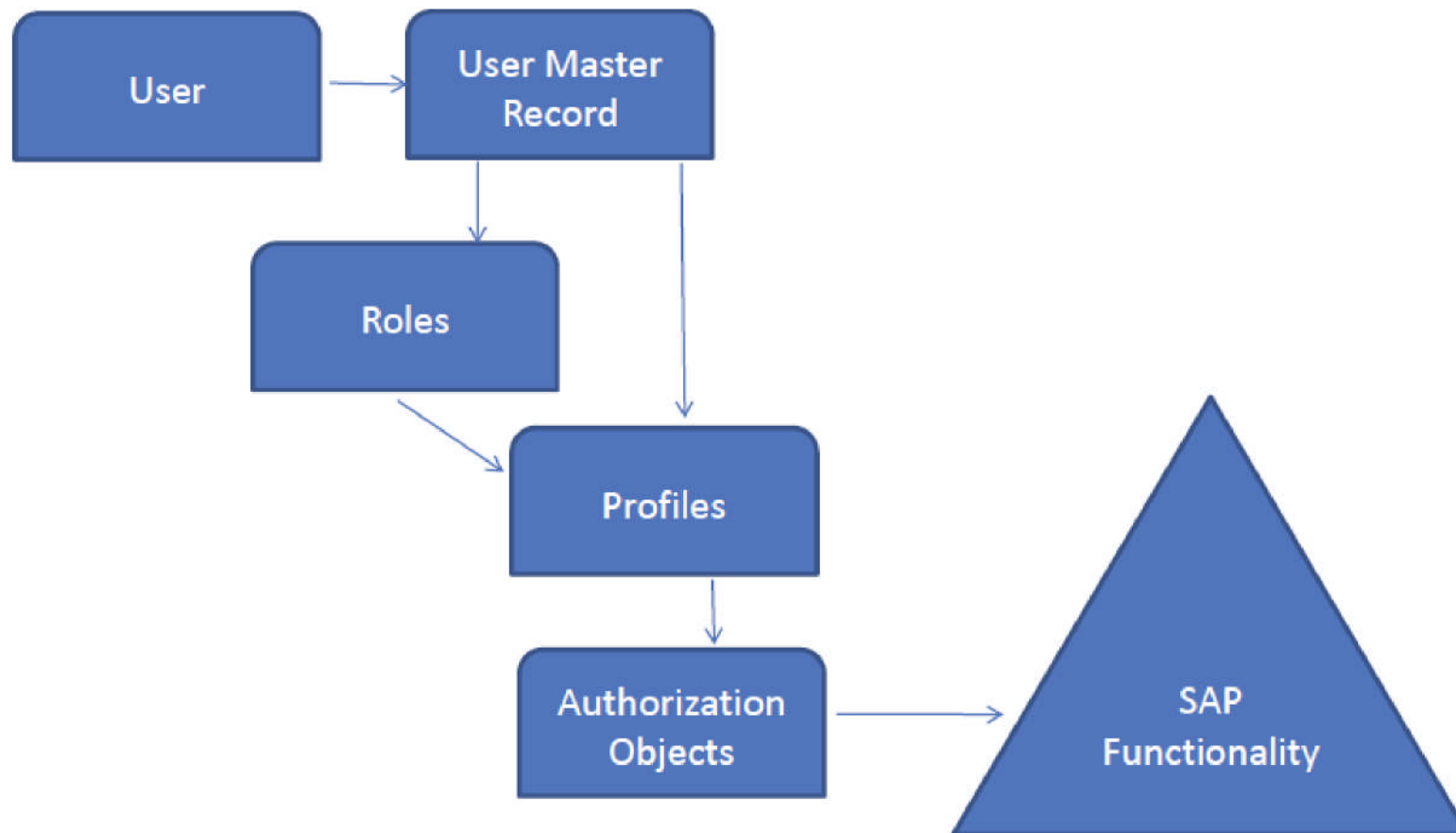
- Users must be setup and roles assigned to user master records before you can use the SAP System.
- A user can only log on to the system if he or she has a user master record.
- User menu and authorizations are also assigned to the user master record via one or more roles.

8.2 Security Architecture

- User Master Record
- Roles
- Profiles – Single and Composite.
- Authorization Objects

8.3 Authorization Concept

Authorization Concept



8.4 User Master Records

- Required to establish access for Users.
- Created when a User is created.
- User Master Records are client-dependent!

8.4 User Master Record Information ... contd

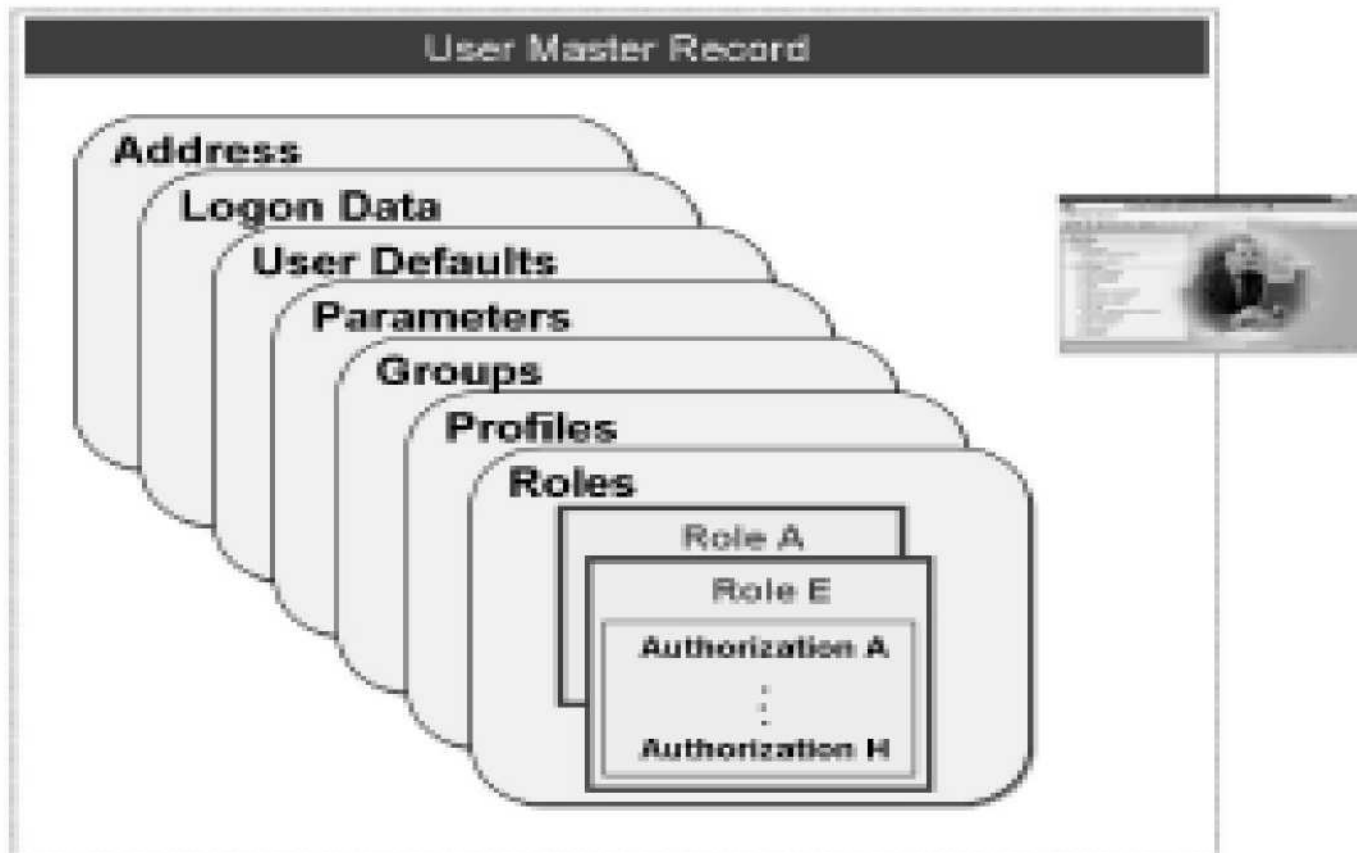


Figure 161: User Master Record

8.4 User Master Record.. contd

User	TEST			Status	Revised
Last Changed On	TEST	03.06.2015	05:29:08		

Address	Logon data	SNC	Defaults	Parameters	Roles	Profiles
---------	------------	-----	----------	------------	-------	----------

Person					
Title	Mr.				
Last name	XYZ				
First name	ABC				
Academic Title					
Format	ABC XYZ				
Function					
Department					
Room Number		Floor		Building	

Communication					
Language	English			Other communication	
Telephone		Extension			
Mobile Phone					
Fax		Extension			
E-Mail					
Comm. Meth	Remote Mail				

Assign other company address...	Assign new company address...
---------------------------------	-------------------------------

8.4 User Master Record.. contd

User	TEST				
Last Changed On	TEST	03.06.2015	05:29:08	Status	Revised

Address Logon data SNC Defaults Parameters Roles Profiles

Alias

User Type Dialog

Password

New Password Rules (Uppercase/Lowercase Must Be Correct)

Initial password

Repeat password

Password Status Product. password

User Group for Authorization Check

User group

Validity Period

Valid from

Valid through

Other Data

Accounting Number

Cost center

8.4 User groups

- Define access to specific users in a group based on role like IT, Finance, etc
- User groups may also reflect the geographical location of the user.
- It is used to restrict the access to specific groups of users

8.5 Type of Users in SAP

- Dialog users (A)
- System Users (B)
- Communication Users (C)
- Service User (S)
- Reference User (L)

8.5 User Types in SAP

User Type		Log on	Password Rules Apply	Change Password
Dialog	A	Dialog Log on	Yes	User & Admin
Service	S	Dialog Log on	No	Admin Only
System	B	No	n/a	n/a
Reference	L	No	n/a	n/a
Communication	C	Comm. Log on	No	Admin Only

8.6 Roles and Profiles

- Roles contain Profiles.
- Profiles contain Authorization Objects.
- Profiles that come delivered with the system or were created from scratch can be assigned directly to users.
- Profiles that were created for a Role are attached to that Role cannot be assigned directly. You must assign the Role and the system will then assign the user the correct Profile.

8.6 Roles in SAP

- Roles are 'built on top' of Profiles and include
 - additional components such as:
 - User menus
 - Personalization
 - Workflow
- In SAP systems, users are typically assigned the
 - appropriate roles by the security team
- The system will automatically add the appropriate
 - Profile(s) for each Role assigned

8.7 Profiles in SAP

- **Authorization are assigned to Profiles for structuring purposes only.**
- **Single profile consists of single or multiple Authorisation.**
- **Composite profile consist of multiple profiles.**

8.8 Examples of Delivered Profiles

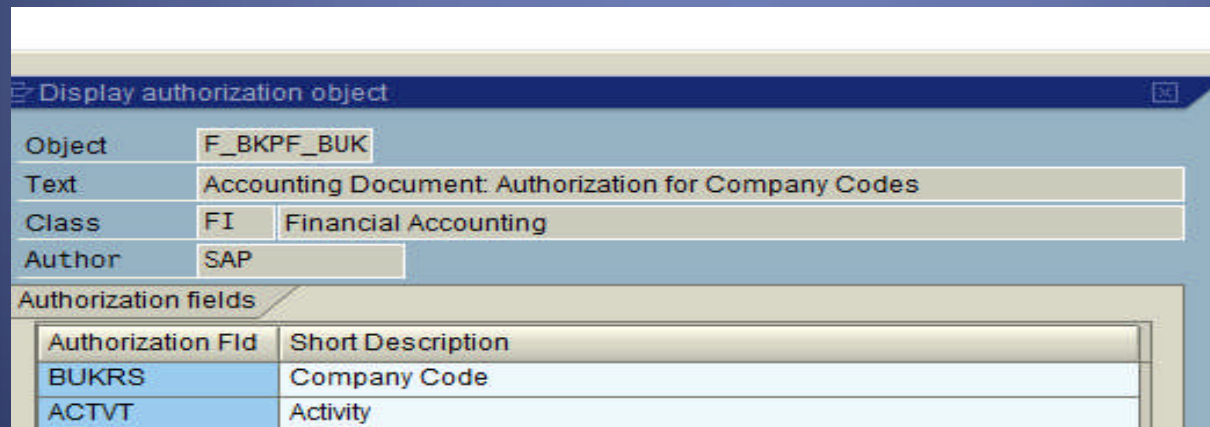
- **SAP_ALL** Delivered with the system
 - Contains almost all Authorization Objects
- **SAP_NEW**
 - Contains the new objects in the current release
 - that are required to keep old transactions functioning.
 - It does NOT contain all new Authorization Objects
 - for that release

8.9 Authorization Objects

- Authorization Objects are the keys to SAP
 - security
- When you attempt actions in SAP the
 - system checks to see whether you have the
 - appropriate Authorizations. (AUTH CHECK Statement)
- The same Authorization Objects can be
 - used by different Transactions

8.9 Authorization Objects

- Example —in order to create, change or display an accounting document, a user must have the Authorization Object F_BKPF_BUK with the appropriate values



The screenshot shows the 'Display authorization object' dialog box in SAP. The object is F_BKPF_BUK, with the text 'Accounting Document: Authorization for Company Codes'. The class is FI (Financial Accounting) and the author is SAP. Below this, the 'Authorization fields' section is expanded to show a table of fields.

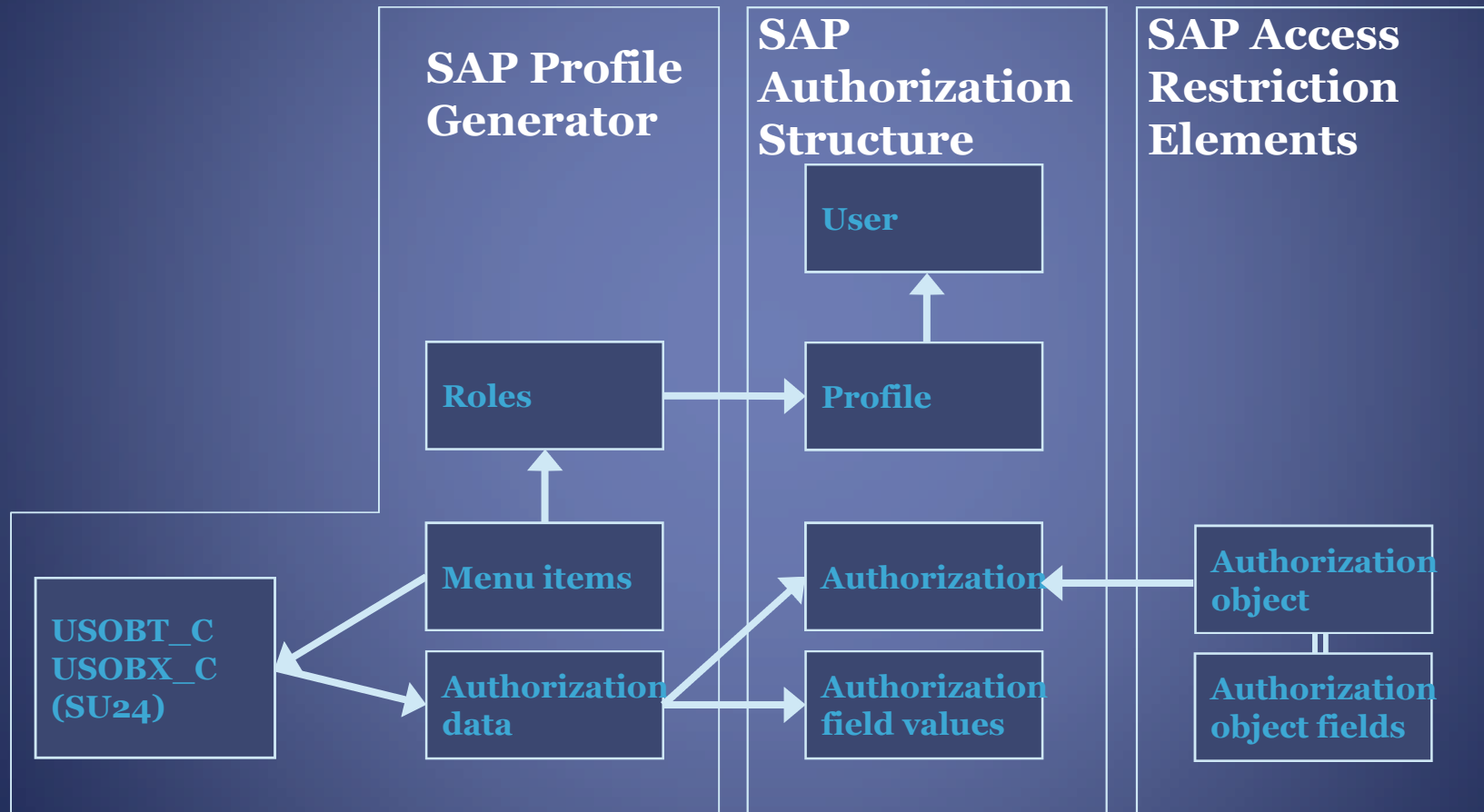
Authorization Fld	Short Description
BUKRS	Company Code
ACTVT	Activity

8.9 Examples of Authorisation

	Example 1	Example 2
Purpose	Create posting for Apple Co.	Change posting for Orange Co
Authorization	Authorization ABC	Authorization XYZ
Value 1	01 (Create)	02 (Change)
Value 2	1000 (Apple Co.)	2000 (Orange Co)

Description	Technical Name	
	F_BKPF_BUK	Authorization Object
Activity	ACTVT	Field 1
Company Code	BUKRS	Field 2

8.10 SAP Structural Security Components



8.10 Profiles and authorisation object.

The screenshot displays the SAP authorization object hierarchy for '2_XM_PUR_PURCHASEORDER'. The tree structure is as follows:

- 2_XM_PUR_PURCHASEORDER (Process Purchase Orders)
 - Standard Cross-application Authorization Objects (AAAB)
 - Maintained Materials Management: Purchasing (MM_E)
 - Maintained Document Type in Purchase Requisition (M_BANF_BSA)
 - Standard Purchasing Group in Purchase Requisition (M_BANF_EKG)
 - Standard Purchasing Group in Purchase Requisition (T-C155070888)
 - Activity Purchasing Group (01, 02, 08) (ACTVT, ENSRP)
 - Standard Purchasing Organization in Purchase Requisition (M_BANF_EKD)
 - Standard Purchasing Organization in Purchase Requisition (T-C155070888)
 - Activity Purchasing Organization (01, 02, 08) (ACTVT, EKDRG)
 - Maintained Release Code in Purchase Requisition (M_BANF_FRG)
 - Standard Plant in Purchase Requisition (M_BANF_WRK)
 - Maintained Document Type in Purchase Order (M_BEST_BSA)
 - Standard Purchasing Group in Purchase Order (M_BEST_EKG)
 - Standard Purchasing Organization in Purchase Order (M_BEST_EKO)
 - Standard Plant in Purchase Order (M_BEST_WRK)
 - Maintained Document Type in Scheduling Agreement Delivery Schedule (M_LPET_BSA)
 - Maintained Purchasing Group in Scheduling Agreement Delivery Schedule (M_LPET_EKG)
 - Maintained Purchasing Org. in Scheduling Agreement Delivery Schedule (M_LPET_EKO)
 - Maintained Plant in Scheduling Agreement Delivery Schedule (M_LPET_WRK)

8.11 User Information System

The screenshot displays the SAP User Information System (SUIS) interface. At the top, there is a menu bar with options: Structure, Edit, Goto, Utilities, Additional Information, System, and Help. Below the menu bar is a toolbar with various icons for navigation and actions. The main area is titled "User Information System" and contains a tree view under the heading "Structure".

The tree view is organized as follows:

- Structure
 - ▶ Cross-System Information (Central User Administration)
 - Users by Address Data
 - ▶ Users by Complex Selection Criteria
 - With Unsuccessful Logons
 - By Logon Date and Password Change
 - With Critical Authorizations
 - ▼ Roles
 - Roles by Complex Selection Criteria
 - By Role Name
 - By User Assignment
 - By Transaction Assignment
 - By MiniApp
 - By Profile Assignment
 - By Authorization Object
 - By Authorization Values
 - By Change Dates
 - ▼ Profiles
 - Profiles by Complex Selection Criteria
 - By Profile Name or Text
 - By Profiles Contained
 - By Authorizations
 - By Authorization Values
 - By Last Change
 - By Role
 - ▶ Authorizations
 - ▶ Authorization Objects
 - ▶ Transactions
 - ▶ Comparisons
 - ▶ Where-Used List

8.12 SAP Security: Transactions

- SU01: Creates and maintains users
- SU02: Creates and maintains profiles
- PFCG: Profile Generator
- SU53: Displays LAST authorization failure
- ST01: Traces keystrokes
- SU03: Lists objects and classes
- SMO4: Monitors user activity
- SE16: can be used to download SAP security tables.
- SU10: Adds or deletes a profile to all users

8.13 SAP Security

- Standard Profiles common to all SAP installations
 - SAP_ALL (unlimited access to system)
 - SAP_NEW (allows older standard profiles to work in newer SAP releases)
 - S_A.SYSTEM: System Administrator
 - S_A.SHOW: Display authorizations only

8.14 Mechanism of Access Control

- User logs onto SAP.
 - User authorisations loaded into the user buffer.
 - User requests transaction directly or through the menu tree.
 - SAP checks if the transaction is blocked.
 - SAP verifies access to the transaction code in the user buffer.
 - Authorisations required read from ABAP program. SAP verifies that authorisations are available in the user buffer.
 - SAP allows user to perform called transaction.
- If any of the above verifications fail – Access is denied.**

SESSION 9

Segregation of Duties

9.1 SOD - Impact on Audit

- Evaluation of SOD is primarily for fraud risk.
- Impact of SODs on automated controls. For e.g. end to end access in Purchase & Payable process.
- Multiple Tcode can perform the same function.
- Assessment of SODs through
 - Tcode —SUIM
 - Tools such as Bizrights, SAP GRC
 - Auditors proprietary tools

9.1 SOD - Impact on Audit — contd..

- Identification of "critical" SODs.
- Identification of compensating controls.
- Business Process Review controls may not
 - address the risk of SOD conflicts.
- Extracting data for such transactions can be done using SAP standard tables.

9.1 SOD - Impact on Audit — contd..

- SOD Analysis is "Point-in-time"
- Profiles also may have changed
- Risk of multiple user id being used by the same person. E.g. Generic user ids, Sharing of passwords.
- Identification of SOD per transaction requires SAP expertise.

SESSION 10

Data Migration to SAP

10.1 Data Migration to SAP

- Data Migration Strategy
- Data Cleansing in Legacy
- Migration dates
- Avoid migration towards the end of the reporting period
- Closing Legacy with new Chart of Accounts

10.1 Data Migration to SAP

- Mapping to new Chart of Accounts and Masters
- Mapping Account Balances, Quantities, Rates, Cost, Accumulated Depreciation, etc.
- Mapping Line Items
- Defining the Go-Live date
- Defining the Black-Out period

19.1 Data Migration to SAP

- Issues on Inventory Movements during Black-out
- Addressing Open PO's Open, SO's etc.
- Uploads through T-Code "LSMW"
- Scrutinize the "Data Migration Account"
- Sign-Offs
- Archival of Legacy

SESSION 11

SAP Upgrade

11.1 SAP Upgrade

- SAP does not support earlier versions.
- All SAP installations will have to move to ECC 6.0
- In a Technical Upgrade, existing functionality is not changed.
 - There is no Data Migration
- In a Functional Upgrade, all business processes and controls will have to be re-assessed for changes.
 - There will be Data Migration.
- There could be modifications to access rights. SODs will have to be assessed again

SESSION 12

Report Validation

12.1 Report Validation

- Reports may be Standard or Customized
- Customized Reports begin with Y or Z
- “System-dependent Manual Controls” also rely on Reports from SAP.
- Identify source of the Report – SAP or BW Report?

12.2 Reports – Impact on Audit

- In case ITGC are reliable -
 - Mere display of tables in SAP does not require validation
 - Logic of Standard Reports may not be validated
 - Logic of Customized Reports (beginning with Y or Z) should be validated, either through white-box or black box testing

12.2 Reports – Impact on Audit contd..

- In case ITGC are not reliable -
 - Mere display of tables in SAP also requires validation, as there is no reliance on underlying data
 - Logic of Standard Reports may also have to be validated.
 - “System-dependent Manual Controls” are based on Reports from SAP. Every Report used for each sample will have to be separately validated.
- Logic of Customized Reports (beginning with Y or Z) should be validated, either through white-box or black box testing, whether or not ITGCs are effective.

12.2 Reports – Impact on Audit -contd..

- Deficiencies noted during performing other audit procedures may have impact on completeness and accuracy of data
- In case of inadequate ITGCs, additional procedures will be required to determine completeness and accuracy of the data
- Some Customized Reports may have to be captured at period-end only – else, data will get over-written
- We may be able to leverage on testing performed by the client
- Ensure appropriateness of Input Parameters

SESSION 13

JE Extraction and Analysis

13.1 Manual JE's – Impact on Audit

- Fraud Risk and Risk of Management Override of Controls
- JE's are either manual or automated
- Non-reliance on Automated Controls – all entries in par with Manual entries
- Substantive audit of manual JE's not practical

13.1 Manual JE's – Impact on Audit – contd..

- All entries posted in BSEG and BKPF Tables
- Roll-forward to ensure completeness of population
- Cut-off to be defined for analysis
- Opening and Closing Trial Balances per SAP need to match up with audited figures

13.2 Manual JE's – Impact on Audit – contd..

- JE Roll-forward and Analysis through use of CAATs
- Maker-Checker rarely used in system
- Identification of “Doc-Types” used for Manual Journal Entries may be incorrect
- Identification of T-Codes used for passing manual entries extremely critical

13.2 Manual JE's – Impact on Audit – contd..

- Criteria for analysis very critical
 - Back-dated entries
 - Transactions passed by IT users
 - Materiality overall and for specific accounts
 - Criteria should be drawn from concepts used in Ledger Scrutiny

Session 14

Other Challenges in SAP

14.1 Other Challenges in SAP

- Absence of printed Books of Account
- Very little “hard-copy” Evidence
- Issues on Data Extraction
- Each SAP installation is unique – Each Company Code is unique
- First-year audits are difficult
- Absence of parallel runs
- Management Perception – SAP does it all
- Audit work-papers

Questions?

THANKS

Our Contacts

- CA Shirish Padey
 - padeysn@yahoo.co.in 9822031689
- Sunit Belapure CISA
 - ssby2000@yahoo.com 9860008621
- CA Chetan Damle
 - chetandamle@gmail.com 9766375580
- CA Gautam Kamat
 - gautam.p.kamat@gmail.com 776 806 3222
- CA Sujay Joshi
 - Joshi_sujay@hotmail.com 9881250208
- CA Niren Desai
 - nirendesai77@yahoo.com 9820846406