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.
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.
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

- Central Database (Storage of all data)
- Access to Database: (Read / Write data)
- Database
- Application: Processing of data using application logic
- Presentation: Presentation of the processed data to the user
- Input / Output of data to users
2.4 Correction and Transport System

- Development
- Change Request
- Quality Assurance
- Production

Moving changes from one R/3 system to another
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-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-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-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

- Remote Function Call
- Application Link Enabling
- Electronic Data Interchange
- Object Linking and Embedding
- Program Interface Communication
- Web Interface
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 needs 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

- Text description (free)
- Address of system (e.g., sapd.umsystem.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

- 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

- SAP Menu
- Favorites
- Buttons
- Command Field
- Application Toolbar
- Navigation Icons
- Title Bar
- Standard Toolbar
- Message Bar
- 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 Organization …..Contd.

• 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]

<table>
<thead>
<tr>
<th>User</th>
<th>Valid from</th>
<th>Valid through</th>
<th>User Type</th>
<th>User Lock</th>
<th>Created On</th>
<th>Last Logon Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>BITRAGNA</td>
<td>00.00.0000</td>
<td>00.00.0000</td>
<td>A</td>
<td>0</td>
<td>10.12.2013</td>
<td>00.00.0000</td>
</tr>
<tr>
<td>CAMPSTME</td>
<td>00.00.0000</td>
<td>00.00.0000</td>
<td>A</td>
<td>0</td>
<td>30.07.2013</td>
<td>00.00.0000</td>
</tr>
<tr>
<td>GARRISLA</td>
<td>00.00.0000</td>
<td>00.00.0000</td>
<td>A</td>
<td>32</td>
<td>23.09.2009</td>
<td>23.09.2009</td>
</tr>
<tr>
<td>02573A7B3F1</td>
<td>18.05.2006</td>
<td>31.12.9999</td>
<td>A</td>
<td>0</td>
<td>18.05.2006</td>
<td>18.05.2006</td>
</tr>
<tr>
<td>0434C129E41</td>
<td>31.03.2006</td>
<td>31.12.9999</td>
<td>A</td>
<td>0</td>
<td>31.03.2006</td>
<td>22.08.2006</td>
</tr>
<tr>
<td>04BFFB8C6607</td>
<td>01.01.1900</td>
<td>31.12.9999</td>
<td>A</td>
<td>0</td>
<td>11.03.2011</td>
<td>03.04.2014</td>
</tr>
<tr>
<td>04F9591D911</td>
<td>10.03.2008</td>
<td>31.12.9999</td>
<td>A</td>
<td>0</td>
<td>10.03.2008</td>
<td>10.03.2008</td>
</tr>
<tr>
<td>08741F8A221</td>
<td>30.06.2006</td>
<td>31.12.9999</td>
<td>A</td>
<td>0</td>
<td>30.06.2006</td>
<td>30.06.2006</td>
</tr>
</tbody>
</table>
5.2 Auditing in SAP
## 5.2 Auditing in SAP

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>User-Defined Value</th>
<th>System Default Value</th>
<th>Parameter Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/min_password_digits</td>
<td>0</td>
<td>0</td>
<td>login/min_password_digits</td>
<td>min. number of digits in passwords</td>
</tr>
<tr>
<td>login/min_passwordlett</td>
<td>0</td>
<td>0</td>
<td>login/min_password_lett</td>
<td>min. number of letters in passwords</td>
</tr>
<tr>
<td>login/min_password_ing</td>
<td>6</td>
<td>6</td>
<td>login/min_password_ing</td>
<td>Minimum Password Length</td>
</tr>
<tr>
<td>login/min_password_low</td>
<td>0</td>
<td>0</td>
<td>login/min_password_low</td>
<td>minimum number of lower-case characters in passwords</td>
</tr>
<tr>
<td>login/min_password_spe</td>
<td>0</td>
<td>0</td>
<td>login/min_password_spe</td>
<td>min. number of special characters in passwords</td>
</tr>
<tr>
<td>login/min_password_upp</td>
<td>0</td>
<td>0</td>
<td>login/min_password_upp</td>
<td>minimum number of upper-case characters in passwords</td>
</tr>
<tr>
<td>login/multi_login_users</td>
<td>0</td>
<td>0</td>
<td>login/multi_login_users</td>
<td>list of exceptional users: multiple logon allowed</td>
</tr>
</tbody>
</table>
5.2 Auditing in SAP
## 5.2 Auditing in SAP

<table>
<thead>
<tr>
<th>Client</th>
<th>User</th>
<th>Lock</th>
<th>Password Status</th>
<th>Reason for User Lock</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>DDIC</td>
<td>Exists; Password not trivial.</td>
<td>Does not exist. Logon not possible. See SAP Note 2383</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAP</td>
<td></td>
<td>Password ADMIN well known. See SAP Note 29276</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAPCPIEC</td>
<td></td>
<td>Password PASSWORD is well known</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TMSADM</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
<tr>
<td>001</td>
<td>DDIC</td>
<td>Exists; Password not trivial.</td>
<td>Exists; Password not trivial.</td>
<td>Locked by administrator</td>
</tr>
<tr>
<td></td>
<td>SAP</td>
<td></td>
<td>Exists; Password not trivial.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAPCPIEC</td>
<td></td>
<td>Password ADMIN well known. See SAP Note 29276</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TMSADM</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
<tr>
<td>066</td>
<td>DDIC</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EARLYWATCH</td>
<td></td>
<td>Password SUPPORT well known.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAP</td>
<td></td>
<td>Password 06071992 well known.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAPCPIEC</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TMSADM</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
<tr>
<td>301</td>
<td>DDIC</td>
<td>Exists; Password not trivial.</td>
<td>Does not exist. Logon not possible. See SAP Note 2383</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAP</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAPCPIEC</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TMSADM</td>
<td></td>
<td>Does not exist.</td>
<td></td>
</tr>
</tbody>
</table>
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
5.3 Auditing in SAP

<table>
<thead>
<tr>
<th>Request/Task</th>
<th>Status</th>
<th>Transport Target</th>
<th>Category</th>
<th>Owner</th>
<th>Date</th>
<th>Time</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D3K90404146</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>CHANDRA</td>
<td>05.05.2006</td>
<td>16:08:08</td>
<td>HR Topline</td>
</tr>
<tr>
<td>D3K90404139</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>SHAHA</td>
<td>05.05.2006</td>
<td>15:43:25</td>
<td>Changes to ZPYXP0_ZSAP_PAYSLIP_DS form</td>
</tr>
<tr>
<td>D3K90404118</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>FITTEN</td>
<td>05.05.2006</td>
<td>23:22:34</td>
<td>Fix MBS budget</td>
</tr>
<tr>
<td>D3K9040408</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>SOHN</td>
<td>11.05.2006</td>
<td>20:19:53</td>
<td>Recruiting Succession for Beth Solomon</td>
</tr>
<tr>
<td>D3K90404049</td>
<td>R</td>
<td>CL5</td>
<td>CUST</td>
<td>C5073548</td>
<td>29.05.2006</td>
<td>21:26:51</td>
<td>Ticket 85133</td>
</tr>
<tr>
<td>D3K90404029</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>CHANDLS</td>
<td>28.04.2006</td>
<td>19:14:51</td>
<td>HR Topline</td>
</tr>
<tr>
<td>D3K903953</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>SOLONOW</td>
<td>27.04.2006</td>
<td>19:35:59</td>
<td>Workbench changes for e-recruiting-BES</td>
</tr>
</tbody>
</table>
5.3 Auditing in SAP

Display View "Clients": Details

Client: 01 IDES Sandbox

City: MUNICH
Logical system: E61CLNT801
Std currency: EUR
Client role: 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
- No changes to cross-client Customizing objects
5.3 Auditing in SAP
5.3 Auditing in SAP

<table>
<thead>
<tr>
<th>User Name</th>
<th>Date</th>
<th>Time</th>
<th>Changed by</th>
<th>Action</th>
<th>Old Value</th>
<th>Text for Value</th>
<th>New Value</th>
<th>Text for the New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABRAHAGE</td>
<td>31.05.2015</td>
<td>23:34:49</td>
<td>MOLLETKI</td>
<td>Lock Changed</td>
<td>128</td>
<td>Incorrect Log...</td>
<td>0</td>
<td>Not locked</td>
</tr>
<tr>
<td>ABRAMEYA</td>
<td>12.04.2015</td>
<td>11:35:22</td>
<td>MOLLETKI</td>
<td>Password Changed</td>
<td></td>
<td>Long Password</td>
<td>Long Password 2</td>
<td>Initial</td>
</tr>
<tr>
<td>AMANGU</td>
<td>10.04.2015</td>
<td>07:06:10</td>
<td>ABRAMEYA</td>
<td>Password status changed</td>
<td></td>
<td>Long Password</td>
<td>Long Password 2</td>
<td>Productive</td>
</tr>
<tr>
<td>AMULYARA</td>
<td>09.04.2015</td>
<td>18:52:51</td>
<td>MOLLETKI</td>
<td>Initial User Type</td>
<td>A</td>
<td></td>
<td>Dialog User</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Password Changed</td>
<td></td>
<td>Long Password</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Password status changed</td>
<td></td>
<td>Initial</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Profile Added</td>
<td>T-EID1000293</td>
<td></td>
<td>Profile for role ZR3_PROJECT...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Profile Added</td>
<td>T-EID1000292</td>
<td></td>
<td>Profile for role ZR3_PROJECT...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Profile Added</td>
<td>T-EID1000291</td>
<td></td>
<td>Profile for role ZR3_PROJECT...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Profile Added</td>
<td>T-EID100029</td>
<td></td>
<td>Profile for role ZR3_PROJECT...</td>
<td></td>
</tr>
</tbody>
</table>
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 likewise 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?

- SAP Application
- SAP NetWeaver / Basis
- Database
- Operating System
- Hardware
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

• Auto Post Indicator
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

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

- Manual Entries to Sales-related accounts
- Sales order – Delivery – Invoice linking
7.3 Purchase - Payables Cycle

- Purchase Order Approval

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

- Unlimited Delivery whether only for scheduling agreement
Tolerances for Quantity and Price

- Absolute
  - Do not check
  - Check limit
    - Value: 1.60

- Percentage
  - Do not check
  - Check limit
    - Tolerance limit %: 2.80

- Absolute
  - Do not check
  - Check limit
    - Value: 3.00

- Percentage
  - Do not check
  - Check limit
    - Tolerance limit %: 4.30
7.3 Purchase - Payables Cycle – contd..

- **Purchase Account Determination**

<table>
<thead>
<tr>
<th>Organization</th>
<th>Plant</th>
<th>Company Code</th>
<th>Chart of Accounts</th>
<th>INT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Valuation Area</td>
<td>Valuation Grpg Code</td>
<td>0001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valuation</th>
<th>Material Type</th>
<th>Material</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
<th>Material Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Movement</td>
<td>Movement Type</td>
<td>101</td>
<td>GR goods receipt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Posting Lines Text</th>
<th>VIGCd</th>
<th>AGC</th>
<th>VC1</th>
<th>PK</th>
<th>Acct Deb.</th>
<th>PK</th>
<th>Acct Cr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gain/loss from revaluation</td>
<td>-e-</td>
<td>-e-</td>
<td>7900</td>
<td>83</td>
<td>232500</td>
<td>93</td>
<td>232500</td>
</tr>
<tr>
<td>Inventory posting</td>
<td>-e-</td>
<td>-e-</td>
<td>7900</td>
<td>89</td>
<td>790000</td>
<td>99</td>
<td>790000</td>
</tr>
<tr>
<td>Incidental costs of external activity</td>
<td>-e-</td>
<td>-e-</td>
<td>-e-</td>
<td>86</td>
<td>415000</td>
<td>96</td>
<td>415000</td>
</tr>
<tr>
<td>External activity</td>
<td>-e-</td>
<td>-e-</td>
<td>7900</td>
<td>85</td>
<td>417002</td>
<td>96</td>
<td>417002</td>
</tr>
<tr>
<td>Change in stock account</td>
<td>-e-</td>
<td>-e-</td>
<td>7900</td>
<td>81</td>
<td>893010</td>
<td>91</td>
<td>893010</td>
</tr>
<tr>
<td>Purchase offsetting account</td>
<td>0001</td>
<td>-e-</td>
<td>7900</td>
<td>46</td>
<td>--Missing--</td>
<td>50</td>
<td>--Missing--</td>
</tr>
<tr>
<td>Purchase account</td>
<td>0001</td>
<td>-e-</td>
<td>7900</td>
<td>46</td>
<td>--Missing--</td>
<td>50</td>
<td>--Missing--</td>
</tr>
<tr>
<td>Materials management exch.rate</td>
<td>-e-</td>
<td>-e-</td>
<td>-e-</td>
<td>46</td>
<td>230000</td>
<td>50</td>
<td>280000</td>
</tr>
<tr>
<td>Cost (price) differences</td>
<td>-e-</td>
<td>-e-</td>
<td>7900</td>
<td>83</td>
<td>231500</td>
<td>93</td>
<td>281500</td>
</tr>
<tr>
<td>GR/IR clearing account</td>
<td>-e-</td>
<td>-e-</td>
<td>-e-</td>
<td>40</td>
<td>191100</td>
<td>50</td>
<td>191100</td>
</tr>
<tr>
<td>Inventory posting</td>
<td>-e-</td>
<td>-e-</td>
<td>7900</td>
<td>89</td>
<td>790000</td>
<td>99</td>
<td>790000</td>
</tr>
</tbody>
</table>
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)
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
7.5 Fixed Assets Cycle

- Account determination
- Depreciation Posting to GL
- 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

- User
- User Master Record
- Roles
- Profiles
- Authorization Objects
- SAP Functionality
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
8.4 User Master Record.. contd
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

<table>
<thead>
<tr>
<th>User Type</th>
<th>Log on</th>
<th>Password Rules Apply</th>
<th>Change Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog</td>
<td>A</td>
<td>Dialog Log on</td>
<td>Yes</td>
</tr>
<tr>
<td>Service</td>
<td>S</td>
<td>Dialog Log on</td>
<td>No</td>
</tr>
<tr>
<td>System</td>
<td>B</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>Reference</td>
<td>L</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>Communication</td>
<td>C</td>
<td>Comm. Log on</td>
<td>No</td>
</tr>
</tbody>
</table>
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.
### 8.9 Examples of Authorisation

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Example 1</th>
<th>Example 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Create posting for Apple Co.</td>
<td>Change posting for Orange Co</td>
</tr>
<tr>
<td>Authorization</td>
<td>Authorization ABC</td>
<td>Authorization XYZ</td>
</tr>
<tr>
<td>Value 1</td>
<td>01 (Create)</td>
<td>02 (Change)</td>
</tr>
<tr>
<td>Value 2</td>
<td>1000 (Apple Co.)</td>
<td>2000 (Orange Co)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Technical Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Code</td>
<td>BUKRS</td>
</tr>
<tr>
<td>Activity</td>
<td>ACTVT</td>
</tr>
<tr>
<td>Field 1</td>
<td>Authorization Object</td>
</tr>
<tr>
<td>Field 2</td>
<td>F_BKPF_BUK</td>
</tr>
</tbody>
</table>
8.10 SAP Structural Security Components

SAP Profile Generator
- USOBT_C
- USOBX_C (SU24)
- Menu items
- Authorization data

SAP Authorization Structure
- User
- Profile
- Authorization
- Authorization field values

SAP Access Restriction Elements
- Authorization object
- Authorization object fields
8.10 Profiles and authorisation object.
8.11 User Information System

- Structure
  - Cross-System Information (Central User Administration)
    - Users by Address Data
    - Users by Complex Selection Criteria
    - With Unsuccessful Logons
    - By Logon Data 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
- SM04: 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

- 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