Auditing in SAP Environment

- CA Shirish Padey
- CA Heta Shah
- CA Mitesh Vora
- CA Kajal Shah
- CA Rakesh Lakhani

ICAI-Mumbai Branch
8th June, 2019
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. Robotic Process Automation (RPA) in SAP
SESSION 1

Introduction to Controls based Audit
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
Questions?
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 140+ countries and has over approx. 437,000 customers in 180+ 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.]

SAP’s Next Big Thing

- R/2 (1979)
- R/3 (1992)
- ERP (2004)
- S/4 HANA (2015)
2.2 SAP - The Product

- R/3 and ERP

- Three tier architecture — Front end (GUI), Application Server, Database Server
2.2 SAP — The Product ..... [Contd.]

- Client — Server Architecture
2.3 R/3 and ERP: Three-Tier Computer

- **Central Database**
  (Storage of all data)

- **Access to Database**: (Read / Write data)

- **Database**
  - Processing of data using application logic

- **Application**
  - Presentation of the processed data to the user

- **Presentation**
  - Input / Output of data to users
2.4 Transport System

- Development
- SAP System
- Change Request
- Moving changes from one system to another

- Quality Assurance

- Production
- SAP System
2.6 Modules in SAP

[Diagram showing SAP ECC 6.0 modules]

- Logistics
- Accounting
- Human Resources
- Cross Applications

- Logistics modules: Sales & Distribution, Material Management, Production Planning
- Human Resources modules: HR, IS
- Accounting modules: FI (Financial Accounting), CO (Controlling)
- Cross Applications modules: PS (Project System), IS (Industry Solutions)
2.6 SAP 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
2.6 SAP 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 SAP Product – features

- SAP 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 and SAP HANA
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
2.8 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
Questions?
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
- PC with SAP GUI

- Internet / Network, VPN
- Connection
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
• Enter Password
• 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

- Title Bar
- SAP Menu
- Standard Toolbar
- Buttons
- Command Field
- Navigation icons
- Application Toolbar
- Favorites
- Message Bar
- Status Bar

Caution:
Depending on your GUI version, the screen may look different even if the SAP version is the same!
Questions?
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
Questions?
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:** USR02  
**Displayed Fields:** 7 of 7  
**Fixed Columns:**

<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_password_lett...</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_hg</td>
<td>6</td>
<td>6</td>
<td>login/min_password_hg</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>000</td>
<td>SAP*</td>
<td></td>
<td>Password ADMIN well known. See SAP Note 29276</td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>SAPCPIC</td>
<td></td>
<td>Password PASSWORD is well known</td>
<td></td>
</tr>
<tr>
<td>001</td>
<td>DDIC</td>
<td>Exists; Password not trivial</td>
<td></td>
<td>Locked by administrator</td>
</tr>
<tr>
<td>001</td>
<td>SAP*</td>
<td>Exists; Password not trivial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>001</td>
<td>SAPCPIC</td>
<td></td>
<td>Password ADMIN well known. See SAP Note 29276</td>
<td></td>
</tr>
<tr>
<td>001</td>
<td>TMSADM</td>
<td>Does not exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>066</td>
<td>DDIC</td>
<td>Does not exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>066</td>
<td>EARLYWATCH</td>
<td></td>
<td>Password SUPPORT well known.</td>
<td></td>
</tr>
<tr>
<td>066</td>
<td>SAP*</td>
<td></td>
<td>Password 06071992 well known.</td>
<td></td>
</tr>
<tr>
<td>066</td>
<td>SAPCPIC</td>
<td>Does not exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>066</td>
<td>TMSADM</td>
<td>Does not exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>301</td>
<td>DDIC</td>
<td>Exists; Password not trivial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>301</td>
<td>SAP*</td>
<td>Does not exist.</td>
<td>Does not exist. Logon not possible. See SAP Note 2383</td>
<td></td>
</tr>
<tr>
<td>301</td>
<td>SAPCPIC</td>
<td>Does not exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>301</td>
<td>TMSADM</td>
<td>Does not exist.</td>
<td></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>DE3K904146</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>CHANDRA5</td>
<td>05.05.2006</td>
<td>16:08:08</td>
<td>HR Topline</td>
</tr>
<tr>
<td>DE3K904139</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 2PYXXF0_ZSAP_PAYSLIP_US2 form</td>
</tr>
<tr>
<td>DE3K904116</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>PITTEN</td>
<td>05.05.2006</td>
<td>23:22:34</td>
<td>Fix MSS budget</td>
</tr>
<tr>
<td>DE3K904068</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>SOHN</td>
<td>11.05.2006</td>
<td>20:19:53</td>
<td>ERercruiting Succession for Beth Solomon</td>
</tr>
<tr>
<td>DE3K904049</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>DE3K904029</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>CHANDRA5</td>
<td>28.04.2006</td>
<td>19:14:51</td>
<td>HR Topline</td>
</tr>
<tr>
<td>DE3K903963</td>
<td>R</td>
<td>CL5</td>
<td>SYST</td>
<td>SOLOMON</td>
<td>27.04.2006</td>
<td>19:35:50</td>
<td>Workbench changes for e-recruiting-BES</td>
</tr>
</tbody>
</table>
5.3 Auditing in SAP
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></td>
<td>23:35:06</td>
<td></td>
<td>MOLLETKI</td>
<td>Password Changed</td>
<td></td>
<td>Long passphrase</td>
<td>Long Password</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Password status changed</td>
<td></td>
<td>Long passphrase</td>
<td>Initial</td>
<td></td>
</tr>
<tr>
<td>ABRAMEYA</td>
<td>12.04.2015</td>
<td>11:35:22</td>
<td>ABRAMEYA</td>
<td>Password Changed</td>
<td></td>
<td>Long passphrase</td>
<td>Long Password</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ABRAMEYA</td>
<td>Password status changed</td>
<td>Initial</td>
<td>Productive</td>
<td>Initial</td>
<td></td>
</tr>
<tr>
<td>AMANGU</td>
<td>10.04.2015</td>
<td>07:06:10</td>
<td>AMANGU</td>
<td>Password Changed</td>
<td></td>
<td>Long passphrase</td>
<td>Long Password</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AMANGU</td>
<td>Password status changed</td>
<td>Initial</td>
<td>Productive</td>
<td>Productive</td>
<td></td>
</tr>
<tr>
<td>AMULYARA</td>
<td>09.04.2015</td>
<td>18:52:51</td>
<td>MOLLETKI</td>
<td>User created</td>
<td></td>
<td>A</td>
<td>Dialog User</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Initial User Type</td>
<td></td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Password Changed</td>
<td></td>
<td>Long passphrase</td>
<td>Initial</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Password status changed</td>
<td>Initial</td>
<td>Profile Added</td>
<td>T-EI0100293</td>
<td>Profile for role Z:R3_PROJECT...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Profile Added</td>
<td></td>
<td>T-EI0100292</td>
<td>Profile for role Z:R3_PROJECT...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Profile Added</td>
<td></td>
<td>T-EI0100291</td>
<td>Profile for role Z:R3_PROJECT...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOLLETKI</td>
<td>Profile Added</td>
<td></td>
<td>T-EI010029</td>
<td>Profile for role Z:R3_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.
Questions?
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?

- 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
Questions?
SESSION 7

Validation of Automated Controls
7. Business Processes

- Period End Financial Reporting
- Order to Cash
- Procure to Pay
- Manufacture to Inventory
- Acquire to Retire
7.1 Period End Financial Reporting

Key sub-processes

- Organization Structure:
  - Client ➔ Chart of Accounts ➔ Company Code
- GL accounting master data:
  - At Chart of Accounts level
  - At Company code level
- Period Maintenance:
  - FI/MM Periods
  - 12+4 periods
  - Account type wise
- Foreign Exchange
  - Exchange Rates
  - Translation accounting
  - Revaluation accounting
- New GL functionality
  - Parallel ledgers,
  - Real-time document splitting

Key T-Codes

FS00 – GL Masters
OB52 – Period Maintenance
OB08 – Exchange Rates
FB01 – Journals processing
7.1 Period End Financial Reporting

Key Automations

- GL marked for deletion and not blocked for posting
- Auto-posting enabled for key GL Accounts
- Document change rules not active for key fields
- Park and Post workflow for Journals
- Automated GL determination for Translation and Revaluation Gain/Loss
- Automated entries classification possible in SAP
- **Inherent controls**
  - Sub-ledger to GL reconciliation automated for Recon Accounts
  - No change possible to accounting relating fields once a document is posted
  - Debits = Credits
  - Some fields are inherently required in a Journal Entry
- Access to maintain periods is restricted
- Access to process / post Journals is restricted
- SOD between Maintain period and process Journals
- SOD between park and post journals in SAP
• Reconciliation Account Type

• Auto Post Indicator
• **Document Change Rule**

<table>
<thead>
<tr>
<th>Field name</th>
<th>BSEG-ZLSPR (Payment Block)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Type</td>
<td>R</td>
</tr>
<tr>
<td>Transaction type</td>
<td>Payments, invoices, credit memos, ...</td>
</tr>
<tr>
<td>Company Code</td>
<td>In all company codes</td>
</tr>
</tbody>
</table>

This master record is blocked ONLY in this Company Code

This master record is marked for deletion ONLY in this Company Code

• **Posting Block**

<table>
<thead>
<tr>
<th>GL account</th>
<th>11390 Work In Process - Roller Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company code</td>
<td>1066 FI Boots - R - Us</td>
</tr>
</tbody>
</table>

Block:
- Blocked for creation
- Blocked for posting
- Blocked for planning

Block in company code:
- Blocked for posting

This master record is blocked ONLY in this Company Code

Foreign Exchange Accounting

- **Chart of Accounts**: CAUS Chart of accounts - United States
- **G/L Account**: 141010
- **Currency**
- **Currency type**

**Exchange rate difference realized**
- **Loss**: 230000
- **Gain**: 280000

**Valuation**
- **Val.loss 1**: 230000
- **Val.gain 1**: 280000
- **Bal.sheet adj.1**: 140099

**Deletion flag**
- **Deletion flag chart of accounts**
  - **Mark for deletion**
- **Deletion flag in company code**
  - **Mark for deletion**

This master record is marked for deletion ONLY in this Company Code
7.2 Order to cash

Key sub-processes

- Organization Structure:
  Client ➔ Company Code ➔ Sales Area ➔ Plant

- Master data:
  - Customer Master Data at Client, Co Code and Sales Area level
  - Pricing master data at Sales Area level
  - Credit Limits

- Sales Orders processing
- Delivery and Post Goods Issue processing
- Sales Invoice processing
- Credit Block and release
- Release of Sales Invoice for accounting
- Receipt of Money
- Ageing of Receivables Review

Key T-Codes
- XD01 – Customer Masters
- VK11 – Price Masters
- VA01 – Sales Order
- VL01 – Delivery
- VF01 – Sales Invoice
7.2 Order to cash

Key Automations

- All Customer Masters are assigned Recon GL Accounts
- Pricing procedures appropriately configured
- Prices not changeable in Sales Orders and defaults from Price Masters
- Delivery requires a preceding Sales Order
- Deliveries cannot be processed in excess of Sales Order quantity
- Sales Invoice cannot be processed in excess of Deliveries
- Appropriate Revenue Recognition
- Prices in Sales Invoice not changeable and defaults from Price master/sales order
- Automated GL determination for Deliveries and Sales invoices
- Automated Rebate processing
- Access to maintain Price Masters is restricted
- Access to release blocked invoice is restricted
- SOD between Sales Order and Delivery and Invoicing
- SOD between Price Masters and Sales orders processing
• Sales Account Determination

![Customer Group/Material Group/Account Key Table]

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

![Specifications for Posting Residual Items from Payment Differences]

• Price Masters changeability

![Condition Type Table]
- **Sales order – Delivery – Invoice linking**

  - Delivery quantity minus Invoice Quantity
  - Quantity is calculated positively
  - Copy price elements unchanged and redetermine taxes
  - Order
7.3 Procure to Pay

Key sub-processes

- Organization Structure:
  - Client → Company Code → Purchase Org → Plant
- Master data:
  - Vendor Master Data at Client, Co Code and Purchase Org level
  - Purchase Info records for Vendor and Materials
  - Material masters
- Purchase Orders processing
- Purchase Order Release
- Goods Receipts processing
- Vendor Invoice processing
- Three way match
- Release of Blocked Vendor Invoices for payments
- Payments

Key T-Codes

XK01 – Vendor Masters
MM01 – Material Masters
ME21N – Purchase Order
MIGO – Goods Receipt
MIRO – Vendor Invoice
F110 - Payments
7.3 Procure to Pay

Key Automations

- All Vendor Masters are assigned Recon GL Accounts
- 3 way match indicators are appropriately set in Purchase Orders
- All Purchase Orders subject to release in SAP
- Goods Receipt cannot be processed in excess of Purchase Order quantity
- Vendor Invoice cannot be processed in excess of Goods receipt
- Prices in Vendor Invoice not changeable and defaults from Purchase Order
- Tabs in invoice for differential amount posting should be inactive
- Vendor not changeable in invoice
- Automated GL determination for Goods Receipts and Vendor invoices
- Duplicate Invoice check
- Automated payments accounting
- Payments to Alternate Payees
- Access to release Purchase Orders is restricted
- Access to release blocked invoices is restricted
- SOD between PO create and PO release
- SOD between Vendor Masters and Payments processing
• Purchase Order Approval

• 3 way match indicators in PO

• Invoice tolerances for 3 way match
- Duplicate invoice Check
- Account determination
7.4 Manufacture to Inventory

Key sub-processes

• Organization Structure:
  - Client ➔ Company Code ➔ Plant ➔ Storage Location

• Master data:
  - Material Master Data – Basic, Accounting, Costing, Plant, Sales Views
  - Bill of Material
  - Routing

• Consumption processing
• Production order processing
• Other goods movements
• Inventory valuation

Key T-Codes

 MM01 – Material Masters
 CS01 – BOM
 CA01 – Routing
 MB01 – Goods Movements
7.4 Manufacture to Inventory

Key Automations

- Inventory valuation method appropriate
- Automated Accounting of goods movement
- All transactions result in value and quantity update
- Negative stock not configured
- No direct changes to material cost
- No use of sensitive movement types like 501/309/561
- Split valuation active
- SOD between Inventory count and posting Inventory count results
- Access to direct changes to Material cost is restricted
- Access to sensitive movements is restricted
Moving Average Inventory Valuation

Standard Cost Inventory Valuation
7.5 Acquire to Retire

Key sub-processes

- Organization Structure:
  - Client → Chart of Depreciation → Company Code
- Master data:
  - Asset Master Data – General, Depreciation Views
- Depreciation Calculation and accounting
- Capitalization, retirement and scrapping accounting

Key Automations

- Appropriate Depreciation configuration
- Automated GL account determination
- Fields in Asset Master data
- Negative Books values not permitted
- Real-time posting and calculation
- Restricted access to Asset Masters and transactions

Key T-Codes

AS01 – Asset Masters
AFAB – Depreciation
AIBU – Capitalization
ABAVN – Scrapping
ABAON – Retirement
ABUMN – Transfer
• Asset Master Data and Depreciation
- Account determination

- Depreciation Posting to GL
Questions?
SESSION 8

Authorization Concept
8.1 Users and Authorization Concept

- 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 User Master Record Information
8.3 Roles and Profiles

- Roles contain Profiles. The system will automatically add the appropriate Profile(s) for each Role assigned.

- Profiles contain Authorization Objects.

- Single profile consists of single or multiple Authorisations.

- Composite profile consist of multiple profiles.

- 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.

- In SAP systems, users are typically assigned the appropriate roles / profiles by the security team.
8.4 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.

- 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.
# 8.5 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>
<th>Authorization Object</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F_BKPF_BUK</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activity</th>
<th>Field 1</th>
<th>Company Code</th>
<th>Field 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT</td>
<td></td>
<td>BUKRS</td>
<td></td>
</tr>
</tbody>
</table>
8.6 Profiles and authorisation object in SAP
8.7 SAP Structural Security Components

SAP Profile Generator
- Roles
- Menu items
- Authorization data

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

SAP Access Restriction Elements
- Authorization object
- Authorization object fields

USOBX_C (SU24)
USOBX_C (SU24)
8.8 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.
8.9 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
Questions?
9.1 SOD - Impact on Audit

**SOD Conflict Risks**

- 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.
- Identification of SOD per transaction requires SAP expertise.
9.1 SOD - Impact on Audit

Key considerations

• 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.

• 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.

• Assessment of SODs through
  · Tcode — SUIM
  · Tools such as Bizrights, SAP GRC
  · Auditors proprietary tools
Questions?
IT Migration

IT Migration
• A process of movement of any one or group of IT Assets from one state of existence to another.

IT Assets
• Hardware, Software, Data, related infrastructure

Data Migration
• A process of moving data from one data structure to another. It is required when any organisation replaces Application or Database system
Objectives of Migration Audit

• Data Integrity
• Control Adequacy
• Business Continuity
• Effectiveness
SAP Migration- Phases

- Vendor Selection
- Process Re-engineering
- Change Management
- Data Migration
Data Migration to SAP - Process

- Determining Source and Target Data Formats
- Data Mapping (Mapping A/c Balances etc.)
- Data Conversion/cleansing
- Business Sign-off
- Data Conversion program
- Test plan and Test Data
- Data Validation and Reconciliation
- Integration Testing
- Promote to Production
- Data conversion Execution
- Data Validation
- Final Signoff by all stakeholders
Data Migration to SAP – Key Points

• Addressing Open PO’s Open, SO’s etc.

• Uploads through T-Code “LSMW” or “LTMC” if migrating to S4 HANA

• Scrutinize the “Data Migration Account”

• Sign-Offs

• Archival of Legacy
SESSION 11

SAP Upgrade
SAP Upgrade

• SAP does not support earlier versions.

• Support for ECC 6.0 will end in 2025.

• Existing ECC 6.0 installations need to Move to SAP S4/HANA.

• 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.
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 -
  – Standard Reports may be relied upon in case of no change in the design/logic of the standard report. Need to establish there is no change.
  – Logic of Customized Reports (beginning with Y or Z) should be validated, either through white-box or black box testing
  – Ensure appropriateness of Input Parameters
12.2 Reports – Impact on Audit -contd..

• In case of inadequate ITGCs, additional procedures will be required to determine completeness and accuracy of the data.

• Generally detailed substantive testing of reports is done to ensure completeness and accuracy of reports.

• We may be able to leverage on testing performed by the client.
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 ITGCs – all entries on 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
- 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
  – Unusual Account Combination/Passed at unreasonable times
Questions?
Session 14

Robotic Process Automation (RPA) in SAP
Automation

What is Automation?

Automation, the application of machines to tasks once performed by human beings or, increasingly, to tasks that would otherwise be impossible

- Encyclopedia Britannica

Benefits of Automation

- Efficiency
- Standardization
- Manual Errors Elimination
- Repetitive Task
Automation Journey

Stages of Implementation

- Awareness
- Process Scanning
- PoC & Governance
- Implementation
- Scaling automation enterprise wide

Technology

- Macro and Scripts
- Business Process Automation
- Robotics Process Automation
- Intelligent Process Automation
RPA in SAP

Why RPA is suited in SAP Environment?
- Stable Environment
- Standardisation
- Rule based

RPA at what level in SAP Environment?

Data Entry/Transaction Level
e.g. Vendor invoice entries in SAP

Reporting Level
e.g. Auto scheduling and emailing of MIS reports

Governance Level
e.g. Configurable controls and Data Analysis testing automation
RPA in SAP

Configurable Controls
- Three way match in ERP
- Duplicate Invoice check etc.

Data Analysis
- Vendors not used for more than 1 year deactivated in system
- Purchase Orders created and released by the same user
- Purchase Order creation/change vs. GRN or Invoice
- Duplicate vendor masters in system
- Potential Duplicate Invoices etc.
THANKS