Risks in ERP implementation
ERP

- A high-end solution featuring integration of information technology and business application.
- Seeks to streamline and integrate operational processes and information flows in the organization to integrate the resources.
- The whole is greater than the sum of its parts.
- Each implementation is unique and is designed to correspond to the implementer's various business processes.
Major functionalities of ERP

- Bridges the information gap across the organisation.
- Facilitates enterprise-wide Integrated Information System covering all functional areas like Manufacturing, Sales and distribution, Payables, Receivables, Inventory, Accounts, Human resources, Purchases etc.
- Helps in eliminating most of the business problems like Material shortages, Productivity enhancements, Customer service, Cash Management, Inventory problems, Quality problems, Prompt delivery etc.
- Provides avenues of continuous improvement and refinement of business processes.
- Helps in laying down Decision Support Systems (DSS), Management Information System (MIS), Reporting, Data Mining and Early Warning Systems to the organization.
ERP and BPR

- Implementation goes closely with business process reengineering and organizational remodelling.
- Understanding the full import of going for ERP; whether enough organizational resilience and flexibility to undertake the project.
- Mismatch between the management aspirations and organizational compliance.
The database is usually centralized and as the applications reside on multiple users the system allows flexibility in customization and configuration.

The processing is real time online whereby the databases are updated simultaneously by minimal data entry operations.

The input controls are dependent on pre data acceptance validation and rely on transaction balancing; time tested controls such are batch totals etc are often no longer relevant.

Since the transactions are stored in a common database the different modules update entries into the database. Thus database is accessible from different modules.
Characteristics

- The authorization controls are enforced at the level of application and not the database; the security control evaluation is of paramount importance.
- Auditors have to spend considerable time understanding the data flow and transaction processing.
- System heavily dependent on networking on a large scale.
- Vulnerability by increased access is a price that is paid for higher integration and faster processing of data in an integrated manner.
- The risk of single point failures is higher in ERP solutions; Business Continuity and Disaster Recovery should be examined closely.
Broad areas to look

- Process integrity,
- Application security,
- Infrastructure integrity and
- Implementation integrity.
Implementation Integrity

- Project Planning,
- Business & Operational analysis including Gap analysis,
- Business Process Reengineering,
- Installation and configuration,
- Project team training,
- Business Requirement mapping,
- Module configuration,
- System interfaces,
- Data conversion,
- Custom Documentation,
- End-user training,
- Acceptance testing and
- Post implementation/Audit support.
To improve operational efficiency, streamline processes and effectively decentralize authority and responsibility - replace the fragmented computerized information systems with an integrated system for global management and administration.

GSM - both a major business change and a major technological change for WHO.
Thousands of WHO staff worldwide are connecting.

Making each country, each region and HQ into identical central points of information has obvious advantages. It means all staff have seamless access to common data. The result is greater collaboration.
Reference Frame

- Oracle E-BIZSuite
- Use of PRINCE2, Oracle AIM, PJM and ITIL by Management
- Audit: CoBIT/SDLC
CoBIT HLCOs for ERP Audit

<table>
<thead>
<tr>
<th>Planning and Organization</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1</td>
<td>Define a strategic IT plan</td>
</tr>
<tr>
<td>PO2</td>
<td>Define the information architecture</td>
</tr>
<tr>
<td>PO3</td>
<td>Determine the technological direction</td>
</tr>
<tr>
<td>PO4</td>
<td>Define the IT organization and relationships</td>
</tr>
<tr>
<td>PO5</td>
<td>Manage the IT investment</td>
</tr>
<tr>
<td>PO6</td>
<td>Communicate management aims and direction</td>
</tr>
<tr>
<td>PO7</td>
<td>Manage human resources</td>
</tr>
<tr>
<td>PO8</td>
<td>Ensure compliance with external requirements</td>
</tr>
<tr>
<td>PO9</td>
<td>Assess risks</td>
</tr>
<tr>
<td>PO10</td>
<td>Manage projects</td>
</tr>
<tr>
<td>PO11</td>
<td>Manage quality</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acquisition and Implementation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AI1</td>
<td>Identify solutions</td>
</tr>
<tr>
<td>AI2</td>
<td>Acquire and maintain application software</td>
</tr>
<tr>
<td>AI3</td>
<td>Acquire and maintain technology architecture</td>
</tr>
<tr>
<td>AI4</td>
<td>Develop and maintain IT procedures</td>
</tr>
</tbody>
</table>
The objectives of the review

- Whether the GSM application development and implementation processes have adhered to the best practices and procedures including governance, risk management and controls.
- Determine the effectiveness of preparedness for the implementation of GSM application.
- The scope was restricted to focus on risks associated with the project processes and preparedness for implementation of GSM project. Other risks associated with IT controls over individual modules or the functionality aspects of GSM were not included.
The focus of audit was on risks associated with project processes and preparedness for implementation of GSM project.

The audit was conducted in accordance with the CoBIT framework.

The key areas of risk identified, analyse these risks and plans for their mitigation.
Areas covered

- Project management
- Contract management
- GSM Budget and staff
- Solution readiness and User Acceptance
- Organizational readiness and training
- IT readiness
- Data conversion, cutover and transition
- System security issues
- Post implementation review
Project management

- Multiple slippages in go-live deadlines
- GSM planning vis-a-vis GSC planning
- Involvement of ITT
- Project Management Methodology
- User Requirements
- Manpower resource
- Total cost of GSM
Project management

- Tolerance
- Involvement of Health Technical Units (HTUs)
- Adoption of International Public Sector Accounting Standards (IPSAS)
- Regression testing
- Parallel testing
Contract management

- Budget and staff
- System Integrator Costs
- Staff Costs
Solution readiness and User Acceptance

- Users’ Acceptance Testing
- Solution readiness for UAT
- Data sufficiency and Quality in UAT
- SIT and UAT
- Test Director Methodology
- E2E scenarios for UAT
- Remediation of Health Technical Units
Organizational readiness and training

- Global Service Centre (GSC)
- Disaster Recovery and Business Continuity Planning for the GSC
- Insurance arrangement for Global Service Centre
- Global Service Desk (GSD)
- Maintaining existing services
- Training
IT readiness

- Knowledge management
- Global Private Network (GPN)
Data conversion, cutover and transition

- Data availability from Businesses
- Loss of Audit Trail
- Quality assurance of the converted data
- Cutover procedures
- Legacy system decommissioning and database archiving
System security issues

- Information Security Management System (ISMS)
- Data classification and patch management
- System security testing
Post Implementation

- Post-implementation review of GSM
Questions?

Dr. Ashutosh Sharma CISA, CIA
AshutoshSharma@cag.gov.in