

2024

ISACA Kenya Chapter

A 2024 Training Programme

[ERP Auditing: Course Outline]

An Enterprise Resource Planning (ERP) implementation and its associated business process changes transform the critical elements of an organization. Prior to ERP systems, an organization's legacy systems were typically organized around functions or departments; for example, sales, purchasing, inventory, and finance, and not around the business processes, such as, purchase-to-pay, and order-to-cash. Functions evolved independently of other functions. ERP systems, on the other hand, have a business process focus. Their 'relational database tables' are designed around a complete set of core functions rather than disparate modules that merely pass transaction data from one module to another. Traditional paper-based audit trails are lost as the internal control structure is transformed to support ERP-enabled business processes. Generally, controls shift from detective to preventive and traditional matching reconciliation controls are automated in the ERP software. Consequently, it makes enormous business sense to ensure adequate controls are properly integrated into the re-engineered ERP-enabled processes.

In the recent past, due to technological advancements, organizations are increasingly moving away from the traditional on-premise ERP systems to 'outsourced' cloud-based ERP implementations. The Auditing function, being a 'third-line' of defense provides assurance to senior management and the board that the efforts by the first-line ('operations') and second-line ('compliance') of defense are consistent with business objectives. So, in outsourced cloud-based ERP implementations, it is critical for organizations to appreciate that while *performance* can be delegated (outsourced), *accountability* (board & senior management mandate) cannot be delegated! The auditing function plays a critical assurance role in cloud-based ERP implementations.

While the computer programs that process data are stored at the Application-level of an ICT infrastructure, the data and information that the programs process and generate, respectively, are stored at the Database system-level. So, in addition to ERP Auditing, this training course is also designed to discuss, at a high level, internal control and security issues surrounding the data stored in various database management systems (DBMS).

This Course Outline highlights the topics to be covered to provide participants with the necessary knowledge required to audit an ERP system, including its data (stored in the database).

ISACA Kenya Chapter

ERP Auditing: Course Outline

Course Duration: Five (5) Days

A. Preamble – National Industrial Training Authority (NITA) Reimbursement:

ISACA Kenya Chapter is registered as a trainer with National Industrial Training Authority (NITA). The Chapter's registration number is **DIT/TRN/976**. Participants from organizations that are registered levy-contributors should apply to NITA for reimbursement of their fees. Please note that this is applicable to Kenyan citizens only and subject to NITA regulations. Remember, to qualify you should apply to NITA for approval prior to the date of the training / conference. Further details can be obtained from NITA website (www.nita.go.ke).

B. Introduction and Overview:

Enterprise resource planning (ERP) is used to denote the planning and management of resources in an enterprise. Secondly, it denotes a software system that can be used to manage whole business processes, integrating purchasing, inventory, personnel, customer service, shipping, financial management, and other aspects of the business. An ERP system typically is based on a 'common database', various integrated business process application modules, and business analysis tools.

ERP systems use data from a wide range of business areas to provide cross-departmental management and process information. The term ERP is no longer about just planning; rather it refers to core critical business processes of an organisation. Thus, in ERP systems, operational and financial data are tied together through a complex information flow. Transactions can be automatically entered without review or pre-checking with the ERP system. Despite the principal usefulness of the concept, ERP system implementations can fail to deliver expected results if not adequately managed and controlled. Further, there are emerging trends and changing technologies that support expanded use of ERP systems (such as, web-enabled customer interfaces, and mobile technologies / devices), which point to the importance of security and control consideration for ERP environments. Thus, the traditional control framework must be extended to include e.g., identity management, content quality, privacy, collaborative commerce, and integrity.

Further, to ensure adequate knowledge and appreciation of the internal controls within an ERP environment, it is necessary that an ERP auditor also understands, at high level, the security issues surrounding the corresponding data stored in various databases (such as Oracle, MySQL, Microsoft SQL Server, IBM DB2, Informix, etc).

The audit of an ERP system requires the Information Systems (IS) auditor to have specific knowledge, and an understanding of the complex features and integrated processes built into and required for the successful implementation, use and control of specific vendor products. The ERP Auditing must, therefore, help organizations better understand fully the risks associated with their ERP systems and the controls that are needed to respond to those risks. Auditors have, therefore, found that they must expand their technological knowledge and skills, devise more effective audit approaches by taking advantage of technology, and design different types of audit tests to respond to new business processes. To become an ERP auditor, one needs to learn ERP concepts (such as SAP, Oracle, JDEdwards, Microsoft Dynamics 365 Business Central, Unit4/Agresso, Sage ERP, and ACCPAC) and Computer-aided Audit Techniques or Tools (CAATs) (such as ACL, and IDEA).

It is noted here that ISACA Kenya Chapter is *vendor-neutral*. So, mentioning the above database management systems (DBMS) and ERP systems are for illustration and example purposes only; and must not be misconstrued to mean endorsement of the systems.

The Training Course will be facilitated by professionals with hands-on ERP audit experience across the globe. It will incorporate facilitated discussions, group discussions, sharing of experiences, and hands-on exercises.

C. Course Objectives:

At the end of this five-day Course, the participants will be able:

1. To understand ERP system concepts, processes, and practices to effectively assess compliance with established policies, standards, and procedures; including laws and regulations;
2. To evaluate the inherent risks associated with an ERP system and the most effective controls that can be designed or configured to mitigate these risks. Critical business processes needed to ensure that an ERP is working in the intended manner and that the system is being adequately controlled will also be discussed in detail;
3. To appreciate that the traditional control measures in an IT environment may not be sufficient to address risks presented by ERP implementation complexities, and emerging technologies such as cloud computing, wireless technologies, and mobile technologies; and
4. To understand, at high level, controls and security issues over database systems (user administration, database administration, operating system-level controls, and database change control).

D. Learning Outcome:

At the end of the training course, participants should have learnt concepts and techniques to able them to:

1. demonstrate understanding of the risks and control issues in an ERP environment;
2. assess ERP systems and recommend improvements for configuration / customization, and usage; and
3. acquire the knowledge necessary to provide ERP audit services in accordance with IS audit standards to assist their organisations with protecting and controlling information systems.

E. CPE Hours Available:

At the end of the course, eligible participants will:

1. earn up to a maximum of 35 CPE (Continuous Professional Education) Hours. This is applicable to those who hold ISACA certification(s) and members of other reciprocating professional bodies; and
2. receive a participation certificate showing the number of CPE Hours.

F. Course Outline (5 Days):

1. Introduction / Overview:

- Understanding Enterprise Resource Planning (ERP)
- Understanding the Business Environment
- Governance, Risk and Compliance (GRC)
- ERP System Implementation / Development
- ERP Audit Fundamentals
- Legal and Ethical Issues for ERP Auditors
- Types of ERP Auditing (e.g., Pre-implementation, post-implementation, Compliance, Process, System, Security, and Waste Audits)

2. ERP Audit Planning: Process Overview

- Risk Assessment
- The Five (5) Planning Steps – ISACA Guidelines
- IT Auditing and Assurance Standards
- Business and / or IT Policies, Standards, Procedures, Processes, and Controls
- Audit Program (Development / Update)

- 3. ERP Audit Fieldwork and Documentation: Process Overview**
 - Overview of Controls over Business Process Cycles (e.g., Procure-to-Pay, Order-to-Cash)
 - Acquiring Data
 - Testing Controls
 - Issue Discovery and Validation
 - Documenting Results
- 4. Audit Reporting and Follow-up: Process Overview**
 - Gathering Report Requirements
 - Drafting the Report
 - Issuing the Report (Executive Summary and Detailed Report)
 - Follow-up
- 5. ERP Implementations and Cloud Computing: Considerations**
 - Cloud Environment: Overview
 - Cloud Migration Security (On-premises to the Cloud, Cloud-to-cloud Migration, and Reverse Cloud Migration)
 - Cloud Deployment Models (Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, and Multi-Cloud)
 - Cloud Service Models (Software as a Service (SAAS), Platform as a Service (PAAS), and Infrastructure as a Service (IAAS))
 - Contractual Obligations (Service Level Agreements (SLA), and Operating Level Agreement (OLAs))
- 6. Auditing General Application Controls**
 - Input Controls
 - Processing Controls
 - Output Controls
 - Interface Controls
 - Master Data Controls
- 7. ERP Internal Control Environment Review**
 - Accuracy, Completeness and Authenticity Checks
 - Processing Integrity and Validity
 - Output Review, Reconciliation and Error Handling
 - Transaction Authentication and Integrity
- 8. Auditing Logical Access Security Controls, Administration, & Change Control (in ERP)**
(To use COBIT® as a reference framework; and Audit Data Analysis Software (CAATs))
 - A Holistic Approach to Password Controls Auditing
 - Risks related to Default User-IDs, Profile Parameters, and Configuration & Maintenance
 - How to Identify Segregation of Duties Control Gaps
 - Identifying Toxic Combinations (SOD Matrix)
 - Interface and Share Folders Controls
 - Auditing End-of-Day Processing – Focusing of High-Risk Areas
- 9. Business Process Risks and Controls (in ERP)**
 - Core Business Processes, including the financial close cycle, the order-to-cash cycle, and the purchase-to-pay cycle
 - Other business process cycles, modules and functions that may be of interest
- 10. Governance, Risk and Compliance (GRC) Solutions**
 - Explore extent of GRC suite of applications (in some ERPs)
- 11. Data Analysis Opportunities**
 - Use Audit Data Analysis tools, such as ACL, and IDEA (*Note: Some ERP systems have their own in-built auditing modules*)
 - Using a sample tool to interrogate the internal control environment of an ERP System

12. Auditing ERP Projects

- Advisory vs. Assurance – Where is Value-Addition?
- Systems Development Life Cycle (SDLC)
 - Requirements Definition
 - Development
 - Testing
 - Solution Implementation
 - Migration – Data Clean-up and Mapping
 - Go-Live
 - Performing Post-Implementation Auditing
 - Risk Management
 - Governance
 - Benefits Realization Business Cases

13. Outsourced IT Environments, including Cloud Computing

- On-premise verses Cloud-based Implementations / Environments
- Auditing Operating Level Agreements (OLAs) / Contract
- Service Level Agreement (SLAs)

14. Auditing Business Continuity and Resilience

- Business Continuity Management / Planning (BCM /BCP)
- IT Disaster Recovery Planning (DRP)
- Data Backup – ISO22301

15. Auditing Database Systems (in relation to Application / ERP Auditing)

- User Administration;
- Database Administration;
- Operating System-level Controls; and
- Database Change Control.

G. Attendance: The training course is designed for internal control professionals and enthusiasts, including the following categories:

- ❖ Application Auditors
- ❖ Internal Auditors
- ❖ Audit Managers
- ❖ Experienced and Up-coming IT Auditors
- ❖ IT Audit Managers / Supervisors
- ❖ Accountants / Finance Professionals
- ❖ IT Audit Consultants
- ❖ Risk Champions
- ❖ Corporate Service Managers
- ❖ IT Professionals
- ❖ Compliance Professionals
- ❖ Audit / Operations Supervisors

H. ISACA Kenya Chapter Secretariat – Contacts:

1. E-mail Address: events@isaca.or.ke
2. Telephone: +254-20-510 0001 / +254-717-116 518 (Office)
3. Jona Owitti, CISA (Chief Trainer, ISACA Kenya Chapter): Mobile Phone: +254-722-742525; e-mail Address: jona.owitti@isaca.or.ke

Thank You.

****** End of the Course Outline ******