SAP ITGC Auditing

Overview

Understanding the core business processes, the integration of SAP applications & system control to optimize the internal control system in order to meet the regulations & international standards. Basic understanding of GRC will also be provided so that participants became aware of latest compliance tool of SAP.

What you will learn

- Impact of the Corporate Governance, SEBI Guidelines, SOX and other auditing standards (for example, ISA) that are relevant for the auditors on the audit process
- Compact overview of the Authorization concept.
- Basic system settings and logs
- Organizational units and organizational structure within an SAP system, Practical analysis of the risks and controls using test cases. General Customizing and controls in Accounting while taking into account the impact on the audit process.
- Auditing of business processes, for example, Procurement, Production, and Sales Order Processing.
- Auditing the end of period financial statements, for example, period- end closing in internal Accounting (Controlling) and in Financial Accounting and Asset Accounting, Evaluation of work in process, allowances, and stock.
- Auditing of specific evaluation methods, for example, stock in an anonymous warehouse, planned cost accounting and inventory costing, actual costing. Transfer of the financial accounting data, balances, and document information to the auditor’s computer in standard format for further analysis (for example, in ACL, IDEA, Excel).
- Protecting the SAP Server from Cyber Attack. Basic overview on SAP GRC along with some Practical's.

Domains (Syllabus)

Control -1 - Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties (SOD).

Control - 2 Access for terminated and/or transferred users is removed or modified in a timely manner.

Control – 3 User access is periodically reviewed.

Control - 4 SOD is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested.

Control – 5: Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company and/or industry standards (such as, password minimum length and complexity, expiration, account lockout).

Control – 6: Privileged-level access (such as configuration and security administrators) is authorized and appropriately restricted.

Control – 7: The key attributes of the security configuration are appropriately implemented.

Control – 8: Application changes are appropriately tested and approved before moving into the production environment.

Control – 9: Access to implement changes into the application production environment is appropriately restricted and segregated from the development environment.