IT and GRC Audit

Inc. TPRA Audit – Practical Approach

100 % Hands-on training with Real life data

TechEd Academy

Learn | Certify | Succeed

Content

About the Course

- 32 Hours (4 Hours X 8 Sessions) of interactive online training
- Watch the Recordings with unlimited views
- **Real-life examples** (Basic to Advance Level)
- Post-training support and career mentorship
- **Interview Preparation** covered in the course
- Support for **CV / Resume building**
- All work-papers (RCM, Checklist, data requirement) will be shared
- Comprehensive hands-on training program that incorporates real-life data to provide practical learning experiences.

Course Outline

01

Scope	Sub-scope
About IT Audit	What is Audit, Type of Audit
Walkthrough	How Walkthrough conducted
	Test of design (TOD) and Test of Effectives (TOE)
Sampling Methodology	How many samples need to pick while doing TOE
	Different sampling techniques
	Automatic Tools for sampling
Information security policy and governance	Review of the existing Information Technology and Information Security policies procedures
	Review the IT strategy and achievement of the same
	Review the allocation of roles and responsibilities
	Review the IT steering committee structure, governance committees and terms of reference
	Review the resource allocation related to IT process including the competencies of the existing staff in line with the responsibilities that they are performing

Course Outline

02

Scope	Sub-scope
Risk Management	Information security Risk assessment and risk treatment procedure
	Review the Risk Register
	Risk Monitoring and Reporting
Exception Management	Exception Request Process, Approval
	Tracking and monitoring of Exception
	Exception Closure and Resolution
User access Management	Review of process of user creation and modification
	Process of User access review
	Review of process of deactivation
	Review of SOD for user access
	Review of Privileged user's activity
	Evaluation of password management controls at DB, and application levels

Course Outline

03

Scope	Sub-scope
Change Management	Review the process of program changes including initiation, documentation, approval, impact analysis, testing and rollback plan
	Review the process of moving to production environment
	Review the process of version control
Incident Management	Incident Management policy and procedure
	Incident Detection and Reporting
	Incident Classification and Prioritization
	Incident Response and Resolution
	Incident Escalation Process
	Root Cause Analysis and Continuous Improvement
	Problem Management
Business Continuity Management	Review the establishment of BCM processes
	Review the Business impact assessment

Course Outline

04

Scope	Sub-scope
Business Continuity Management	Review the completeness of disaster recovery plan including the testing
	Review the controls of the disaster recovery site and business continuity site
	BCP/DR testing and documentation
Vulnerability Assessment and Penetration Testing (VAPT)	Review of internal process for conducting VAPT and source code review and tracking close of vulnerabilities
	Process review of the API Performance Monitoring
Audit Log Management and Monitoring	Adequacy of audit logs for user activities, master management and critical management
	Monitoring of critical audit logs of application and database
	Review of logs using SIEM
Human Resource security control	Pre-employment Security Screening
	Employment Contracts and Confidentiality Agreements
	Security Training and Awareness
	Termination and Offboarding

Course Outline

05

Scope	Sub-scope
Capacity management	Review of capacity monitoring parameters and thresholds defined
	Review of capacity monitoring for critical systems for projections of future capacity requirements
Assets Management	Review Assets Onboarding process
	Review Assets register and tracking process
	Review of hardening process and documentation of hardening/ baseline configuration setting
Patch Management	Patch Identification and Categorization
	Patch Testing and Patch Deployment
	Patch Monitoring and Reporting
Backup and Restoration	Review of the process of defining the data backup requirements
	Storage and Retention of Data Backups
	Review of Restoration Process of data backups (policy, schedule, user requirement, and testing)

Course Outline

06

Scope	Sub-scope
Input, Processing, and Output Controls	Evaluation of the Application controls, testing for effectiveness
Network Security	Review of hardening process and documentation of hardening/baseline configuration setting
	Review of firewall rule review
	Review of user access management on network devices
End point Security controls	Data Loss Prevention (DLP)
	Antivirus Solutions
	Virtual Private Networks (VPN)
	USB and Peripheral Port Control
	Mobile Device Management (MDM)
	Privileged Identity Management (PIM) tool
Data security Controls	
Physical and Environmental security controls	

Course Outline

07

Scope	
Review Data Classification Procedures	
Cyber Security Policy and procedure	
Overview of ISO 27001, ISO 22301, and ISO 27701	
TPRA Audit (Next slide)	
Audit Report preparation	
Interview preparation	
Resume building guidance	

Course Outline

08

Scope of TPRA Audit
Review of Third-Party Risk Management Framework
Review of Vendor Onboarding process, Vendor monitoring, and offboarding
Review of Business objectives, governance, and security risk management practice
Review of data protection and access management process
Review of application management, Application security management, and escrow arrangements in case of application ownership
Review the process of monitoring compliance with IT and IS Policies
Review of Incident Monitoring, Response, and Reporting
Human Resource Security controls related to screening, NDA, disciplinary process
Review of Security Controls for endpoints like antivirus, patching, password, and logical access controls
Review of the process of user creation, deactivation, and modification
Review of Data Leakage Controls
Review the training calendar and program on security awareness conducted
Review the service organizational controls with focus on the services provided by the third party
Evaluate infrastructure resiliency plan and crisis management plan
Review of BCP / DR testing and documentation
Review of hardening process and documentation of hardening/baseline configuration setting for systems
Review the process for firewall rule review
Review of sample network device hardening review

Know your Trainer

SACHIN HISSARIA

CA, CISA, CEH, DISA, COBIT-19, CC-ISC2, RPA

- There is no bigger teacher than experience, Sachin has spent a decade in the field of information security audits and still actively contributing to the field
- Expertly guided countless professionals to **secure Job in Audit domain**
- **CAG empaneled trainer**
- Conducting various other trainings like IT and GRC Audit, NIST CSF 2.0 training, and ISO27001 for corporates and training institutes

in/sachin-hissaria

@Sachin_hissaria

Type of Audits Covered

- ✓ ITGC Audit
- ✓ ITAC Audit
- ✓ TPRA Audit
- ✓ IT security Audit
- ✓ IT Governance Audit
- ✓ SOX Audit
- ✓ Overview of SOC 2 Audit

Who Can Join?

- ✓ Anyone interested in IT and IS Audit
- ✓ Qualified IT Professionals (like CISA, CISM, ISO27001, etc.) who want to learn practical aspects of IT / IS Audits
- ✓ Chartered Accountant & Article Assistant who wants to make their career in IT Audits

Pre-Requisites

- ✓ The course is tailored for individuals new to the field who have an interest in IT Audit. Basic knowledge of MS Office (Excel, Word, PowerPoint) is necessary for data analysis and report preparation.

Contact Us

Want to know more about the course?

+91 88302-38589

https://www.techedacademy.com/it-grc-audit

support@techedacademy.com

Visit our website to know the Current Live batch details
Or
Contact us for Registration

www.techedacademy.com

TechEd Academy
Learn | Certify | Succeed