

Resume

Naresh. P

Contact: +91 8142995229

Email: pnaresh1566@gmail.com

SUMMARY

- Having 3.4 years of experience in ITGC, ITAC, SOX404, Identity and Access Management, Access Reviews, Computer Operations and experienced IT Auditor
- Responsible for the timely conduct of half-yearly cyber security audits and system audits as per regulatory guidelines. Getting RCA for IT-related incidents and reporting to Management on a monthly basis.
- Worked around ITGC controls like Change Management, Access Management, and Manage IT operations and worked on controls like Patch Management, Incident Management, Asset Management, BCP.
- Assisting the client's internal audit team in identifying gaps in the IT control environment for all in-scope business processes and underlying IT applications and infrastructure.
- Complete testing of controls in a highly compressed schedule, which helps clients in meeting regulatory deadlines.

EDUCATIONAL QUALIFICATION:

BTech from LPU in 2020

EXPERIENCE:

SBI-SG Global Securities Services Pvt. Ltd — Dec 2023 to Sep 2024

Assistant Manager

Responsibilities:

- Performed various reviews of general IT controls, system access security, and application system controls to ensure the processes and data are in compliance with the Information Technology and Information Security Policy and Regulatory requirements.
- Responsible for the timely conduct of half-yearly cyber security audits and system audits as per regulatory guidelines. Getting RCA for IT-related incidents and reporting to management on a monthly basis.
- Timely closure of VAPT Points, assessing the report and coordinating with the IT team before the regulatory timelines.
- Preparation of IN- Principle and financial note for Information security related projects and getting it approved from Management.

- Ensure adherence/rectification of observations of external IT/ IS Audits and closure of Audit Reports.
- Interacting and coordinating with various teams for Security and compliance-related audits.
- Implementation of ISO 27001:2013 at organization level.
- Responsible for timely submission of IT/ IS risks issues/observations to Senior Management for review.
- Implementation of Endpoint and Email DLP at the organization level.
- Carrying out Internal committee meetings like the Internal Risk Management Committee, and Information Security Management Steering Committee and recording the minutes.
- Updating IT and IS Policies on an annual basis as per the guidelines received from Regulatory and other CERT-IN empanelled audit firms.
- Carry out Phishing simulation on a monthly basis and tracking of records to present to Management.
- Provide knowledge and guidance of SEBI circulars related to IT controls and remain abreast of emerging trends and best practices in the industry.
- Conducting information security awareness sessions for employees.

ACCENTURE

June 2021 — December 2023

IT Analyst

Responsibilities:

- Performed mainly on Access management, and Change management - SOX-404 and including IT General Controls.
- Working from the Initial phases of the audit from planning & doing the fieldwork & preparing reports and documentation to doing follow-ups to make sure remediations are being implemented.
- Performing Test of Design (TOD) & Test of Effectiveness (TOE) of the controls.
- Performed Identification of risks by testing the controls (ITGC), Problem management, Backup and recovery, and Asset Management.
- Performed internal audit for Access reviews for highly privileged user accounts (HPA) and Non-highly privileged user accounts (Non-HPA) for Applications and Servers.
- Performed Quarterly HPA, User Access creations, User Access Terminations, User Access Reviews, Password configurations, and testing of other controls, finding observations and providing necessary remediations.
- Worked directly with application owners to gather the information related to performing audit and verifying the completeness & accuracy of the data provided.
- Execute daily, and weekly checks to ensure access is terminated for exited users within the organization.

- Worked on Controls like Patch Management, Incident Management, Asset Management, Business Continuity Plan, etc.
- Collecting the evidence by coordinating with multiple teams and thereby reviewing & securing them.
- Identify the appropriate stakeholders and perform interviews, walkthroughs, and documentation reviews to gain an understanding of the processes and documented work papers for ITGC.
- Experience in SOC Reports.
- Knowledge on ISO27001.