

CHANDRALEKA

leka.chandra@gmail.com | +91 9962133622

LinkedIn: [linkedin.com/in/chandrалека/](https://www.linkedin.com/in/chandrалека/)

PROFESSIONAL SUMMARY

Certified Information Systems Auditor (CISA) with over 10 years of experience in IT audit, cybersecurity, risk management and infrastructure management.

Experience in conducting audits and risk assessments aligned with standards (ISO 27001, NIST, GDPR, SOX, DORA, PCI DSS) and evaluating cybersecurity postures across cloud, application and infrastructure. Proven track record in delivering risk insights, improving control environments, driving compliance and deliver strategic insights to stakeholders with work experience in Singapore, Malaysia, United Arab Emirates and India. (Immediate Joiner)

CERTIFICATIONS

Certified Information Systems Auditor (CISA) – ISACA (April 2018)

PROFESSIONAL EXPERIENCE

Assistant Manager – IT Audit & Security - **FLEX, Singapore**

Nov 2022 – May 2024

- Lead and manage the IT audits covering infrastructure systems and enterprise applications.
- Evaluate ITGC and application controls focusing on user access management (creations, terminations, transfers), change management, batch job, privileged user access review, physical security and password controls.
- Review the SDLC (Software Development Life Cycle) process and identify gaps in the software development practices.
- Review disaster recovery and business continuity process for critical systems.
- Lead audits and conduct risk assessments related to data security and privacy controls.
- Deliver actionable insights to senior leadership using GRC tools on remediation plans (MAP – management action plans) and control enhancements.
- Prepare detailed audit report on rating, issue, impact, risk, control and document the results of substantial testing adhering to COBIT Standards.
- Lead and manage compliance testing across key IT systems including active directory, windows, unix, oracle, AWS cloud and applications (Oracle NetSuite, Service Now, SAP Business, Web methods, Infor Baan, Oracle BO etc).

- Travel to office locations based on business requirements(India, Malaysia, United Kingdom, Singapore and Ireland).
- Lead IT audits covering AWS cloud, IAM policies and cloud-native security controls.
- Conduct firewall audits (Fortinet, Palo Alto) including rule base analysis, unused rule identification and access review.
- Execute audits across third-party vendors which includes review of SOC reports, bridge letters (SSAE) attestation.
- Review the cyber security controls across the financial applications for encryption, role-based access control (RBAC), MFA, vulnerability scans, Segregation of duties conflict (SOD) and patch management.
- Conduct third-party risk reviews including Information produced by the entity (IPE) and Information used in control (IUC) testing to validate data accuracy and reliability in the audit processes

Senior IT Auditor - FLEX, Malaysia

Jan 2019 – Oct 2022

- Manage the cybersecurity governance and risk management process across the organization.
- Review SOC Reports (SSAE Type 1, Type 2) and bridge letters for third party systems.
- Manage and review the endpoint security review controls (antivirus, patching, baselining, hardening and group policy)
- Review the report of vulnerability scan from Nessus tool and assess the mitigation strategies.
- Execute IT Risk assessments for disaster recovery and business continuity plans to ensure organizational resilience and compliance.
- Conduct IPE/IUC testing to assess the effectiveness and reliability of the reports generated for the audit.
- Perform security audits focusing on network infrastructure (firewalls, routers, switches) and evaluate the effectiveness and reliability of internal controls to drive continuous improvement in the IT governance.
- Review and participate in Disaster Recovery (DR) drills, including simulation, parallel Testing, and full interruption resting to evaluate system resilience and business continuity effectiveness.
- Evaluate the effectiveness of software whitelisting policies to validate only authorized software's installation on the endpoints and servers.
- Review the reports from endpoint protection software to monitor for data leakage and assess BYOD restrictions.

Senior Engineer – Card Systems Middle East, Dubai

Feb 2016 – Apr 2017

- Facilitate and collaborate with external auditors, administrators and end users to maintain robust security and compliance standards
- Conduct comprehensive assessments of information systems and evaluate the effectiveness of controls by executing IT general controls and application controls audit.
- Analyse and refine documentation process flows and reporting mechanisms to optimize IT control review processes
- Configure and manage web servers and review the vulnerability scanning results
- Lead incident response efforts for IT outages and security breaches
- Create runbooks with standardized procedures for handling IT incidents, disaster recovery (DR) and business continuity processes.

Senior Engineer – IPROTECS Solutions, India

Sep 2012 – Oct 2015

- Manage Physical servers and virtualization (VMware) environment
- Integrated Active Directory with enterprise services and administer endpoint security tools.
- Develop and maintain scripts for automating administrative tasks and improving system efficiency.
- Deploy and manage virtualization technologies including VMware and ensure systems security by applying patches and system configuring security settings.
- Manage and maintain Windows server environments by ensuring high availability and optimal performance by configure Microsoft clustering, active directory and domain controllers.
- Document and refine post incident analysis and corrective actions.

Senior Engineer – **Flextronics Global Shared Services, India**

Jan 2009 – Oct 2011

- Enforce and optimize identity and access management (IAM) including role-based access control (RBAC), multi-factor authentication (MFA) and privileged access controls.
- Monitor, detect and respond to security incidents using SIEM, endpoint protection, and threat intelligence platforms.
- Assist in the planning and execution of server migrations, upgrades for server commissioning and decommissioning.
- Administer windows servers and active directory and implement group policies for secure infrastructure.
- Perform data restoration test on a quarterly basis to evaluate the adequacy of Business continuity process.

Engineer – Systems -**Wipro Technologies, India**

Jun 2007 – Nov 2008

- Configure and manage DNS,DHCP,webservers and active directory.
 - Install and maintain domain controllers and ensure the replication of directory data across domain controllers.
 - Execute Microsoft monthly patch management process to update security patches on the end user's computers and servers.
 - Perform routine backups and restoration test to support disaster recovery efforts
 - Provide technical support to end users resolving issues with hardware software and network connectivity.
 - Implement Active directory group policies to enforce security standards and streamline administrative processes for password and computer policies.
 - Monitor the incidents and resolve within the defined Service level agreements (SLA).
-

CAREER BREAK

May 2024 – Present

- Took a planned career break to manage family responsibilities while continuing self-development and skill enhancement.
 - Continue to upskill professional development courses in Cloud Security, CISSP Training and ISACA webinars.
-

EDUCATION

- Master of Science – Bharathidasan University, India (2007)
 - Bachelor of Science – Bharathidasan University, India (2005)
-