Arun Prakash

Cyber Security

Contact

Address
Bangalore, IN 560049

Phone
8826175495

E-mail
arunprakashnokia@gmail.com

Skills

Cyber Security GRC, Cloud Security Compliance, CASB (Cloud Access Security Broker), AWS security, Risk Management, Security Metric, Third Party Risk Management, GDPR, Information Systems Audit, Incident Management, Application Security and secure system development lifecycle, CISA, ISO 27001, PCI DSS

Dedicated and seasoned Cyber Security professional with 15+ years of experience in all aspects of cloud security and compliance, Cyber security strategy, Governance Risk and compliance, IT and Cyber security Audit, Enterprise Cyber Security Risk Management, Vendor Risk Management, Change Management. Posses strong analytical skills to solve problem quickly and add value to stakeholder relationships, both internal and external to an organization.

Work History

2022-09 - Current

AVP- Cyber Security

Standard Chartered Bank, Bangalore
Information Cyber Security (ICS)

- Risk Assessment: Conduct risk assessments to identify and prioritize information security risks within the business unit, considering factors such as data sensitivity, threats, vulnerabilities, and potential impacts
- Vulnerability Management: Reviewing vulnerabilities' data from multiple sources (i.e. external / internal penetration testing, internal / external vulnerability scanning, etc.) across multiple technologies and a changing environment including infrastructure and applications to determine risk rating of vulnerabilities to business assets.
- Security Controls: Implement and maintain appropriate security controls, policies, and procedures to mitigate identified risks and safeguard information assets, including data classification, access controls, encryption, and monitoring
- Vendor Risk Management: Assess the security posture of third-party vendors and service providers used by the business unit, and ensure that appropriate security controls are in place to protect shared data and resources
- Security Metrics: Develop and maintain security metrics and key performance indicators (KPIs) to track the effectiveness of information security controls, report on security posture, and support

decision-making
- Perform Internal Assessment against various Standards to ensure established policies are being followed and prepare internal reports.
- Security Awareness: Promote security awareness and best practices among employees within the business unit through training, communication campaigns, and ongoing education initiatives
- Detailed understanding of SOC reports (SOC2, Type 1, 2), ISMS reports and ability to relate IT General Controls, IT Application Controls, Cyber Controls to SOC framework.
- Expertise in understanding business impacts of technology decisions as they relate to cloud adoption and enablement, specifically risk management and security.
- Work with Cross functional teams like Engineering, Infrastructure, IT, Legal and help minimize security risks.

2018-07 - 2022-08

Principal Engineer- Infosec

Acuity Knowledge Partners, Bangalore
Information security/ IRM/Cloud compliance:
- Compliance and Governance of Vulnerability Assessment/Penetration Testing
- Information Security Risk Management (Extensive experience within information security& risk function, with assessment, treatment plan and governance)
- Deployment and Implementation of the GRC tool
- Perform IT Audit reviews in areas of SOX (Process), SOC -2 Audits, ISO27001.
- SIEM review and monitoring
- Conduct Third Party Risk Assessment and Vendor Assessment before on boarding.
- Maintain Cloud Security program to determine compliance to Cloud Security policies and industry frameworks like CIS Benchmarks, NIST etc.
- Respond to RFP/RFI questionnaires.
- SOC2 Type II review and compliance.
- GRC Implementation: Work on GRC portal (in house) roll out from scratch till go live.

2015-08 - 2018-07

Senior Consultant- Cyber Security

Capgemini, Bangalore

Information security/ IRM:

- Information Security Risk Management - Conduct assessment of risks to information assets and risk mitigation activities to safeguard organizational assets.
- Conduct Internal Audit based on ISO27001, PCI DSS and other security framework
- Vulnerability Assessment/Penetration Testing
- Performing third party risks assessment on behalf of our clients over the outsourced processes
- SOC2 Type II review and compliance
- Development and review of Information Security policies and procedures
- Respond to customer risk or due diligence questionnaires
- Collect data for the Security metrics and report the same

Cloud Security compliance and governance:

- Identify the unapproved & high risk cloud services and work with proxy team to splash and block these services
- Assist Cloud service owner/Contract owner for CSAR (Cloud service acquisition request) process
- Identity and Access Management – CASB tool
- Risk analysis of cloud services (SAAS & IAAS) through Skyhigh(McAfee) tool
- Governance and Risk Management
- Cloud Service Availability and Operational Resilience
- Cloud Access Control & Identity Management
- Cloud Audit Logging and Intrusion Detection

2013-09 - 2015-07

Assistant Manager- Infosec

Jabil Global Service, Gurgaon

· Ensure services are provided in accordance with ISO 27001: 2013 standards

· Perform VAPT activities

· IT Risk assessment

· Identity and Access Management (IAM),

· SOC2 Type II review and compliance

· Maintain necessary documents and records to satisfy the requirements of ISO 27001

· Perform Internal Audit based on ISO27001 standard

· Conduct information security training and awareness of all staff and ensure compliance to

security quiz
· Security incident management (identify security events / incidents, conduct investigation, gather evidence, report to relevant authorities, suggest preventive measures and closures)

2009-10 - 2013-09	**Consultant Engineer- Infosec**

Sasken , Bangalore
· Conducting periodic security risk assessments on existing systems and identifying and/or recommending appropriate security counter measures and best practices to ensure compliance.
· Perform control assessment and ensure mitigation of gaps by effective governance and stakeholder engagement
· Conducted ISO 27001 Internal Audits.
· Creating policies, standard and other process
· Vulnerability Assessment for Servers, desktops and Network devices

2008-10 - 2009-09	**QA Analyst**

Nokia Siemens Network, Kolkata
· Internal Quality Audit
· RCA/Corrective action
· Implementation of TL9000 requirement & Measurement

Education

High School Diploma

Purnia College - Purnia

2007-06	**BE: Electronics And Communication**

Rajiv Gandhi Proudyogiki Vishwavidyalaya - Bhopal

Certifications

ISO 27001, PCI DSS, AWS security engineering, CISA,ISO20000, TL9000