Bengaluru, India 560034

07349104541

hemadamini6@gmail.com

PROFESSIONAL SUMMARY

14 years of experience in IT, Quality assurance and Compliance and has worked in mid-level management position in the areas of: Business & Process excellence Consulting, IT governance & advisory, Risk management, Business-IT alignment, Audit & Compliance Management, Service Delivery Assurance, Business Continuity & Disaster Recovery Management, Consulting. Worked in with SIEM Tools and with vulnerability assessment and penetration testing.

CORE QUALIFICATIONS

- Risk Assessment Gap Analysis ISO27001
- GDPR
- GRC (Governance, Risk & Compliance
- Web Application Penetration Testing
- Vulnerability/Security Tester cloud Security
- Compliance SOC1 &SOC2
- Disaster Recovery Planning
- Security plan development
- Compliance investigations
- Internal and external audits
- Azure AZ-500
- Aws security specialty
- GCP (cloud digital Leader)
- CISSP (pursuing)

Hemalatha Ponnusamy

EXPERIENCE

March 2022 - Current

Cloud Security &Resilience Manager Hcl Technologies

Designed, implemented, and continually improved compliance programs, effectively addressing key risks, and ensuring alignment with ISO/IEC 27001, SOC2, PCI, NIST, and FedRamp frameworks.

Collaborated with Engineering, Product, Cloud Security, Legal, Privacy, and Corporate Security teams(ISMS Team) to develop pragmatic solutions to complex security risks and compliance issues.

Played a pivotal role in enhancing internal policies, processes, and overall security governance, contributing to a more secure operational environment.

Drove automation initiatives and assisted in the successful adoption of GRC tools, streamlining compliance management and increasing operational efficiency.

Conducted technical gap assessments and risk assessments, proactively identifying vulnerabilities, and recommending solutions.

Facilitated control monitoring activities, ensuring ongoing compliance and swift detection of policy violations.

Collaborated closely with Cloud Security teams to address initiatives and risks affecting the designated area of responsibility.

Identified opportunities to create positive impacts on activities and achieve operational efficiencies.

- Maintained and optimized security compliance monitoring and alerting systems, providing expert advice to control owners regarding system policy violationsMeeting with clients to discuss their security needs and satisfactionwith Azure services.
- Using internal resources from Microsoft and external resources to develop security measure.
- Designing additional security features, such as access management tools
- Analyzing existing cloud platforms and performing threat simulations to spot security vulnerabilities
- Develop and implement an IAM program with policies and procedures.
- Manage user access to systems, applications, and data.
- Monitor compliance with policies, regulations, and customer requirements.
- Perform risk assessments and audits.
- Develop and implement an IAM program with policies and procedures.
- Manage user access to systems, applications, and data.
- Monitor compliance with policies, regulations, and customer requirements.
- Perform risk assessments and audits.
- Comply with information security processes, procedures, and controls Design and develop IAM services and tools
- Customize IAM product features to fulfill requirements that cannot be met with standard out-of-box functionality
- Perform vendor and technology assessments

July 2021 - December 2021

Risk Officer Wipro Technologies

- Consult with relevant units to determine, quantify, and mitigate risks involved in establishing and maintaining various client and industry relationships.

Assessed metrics and monitoring procedures.

- Conduced various security assessments
- Provide advisory consulting by providing suggestions and solutions to the customer problems Reviewed several IT projects for security.
  controls that can or need for enhancements.
  Provide Documentation and Implementation
  Support End-to-End Consulting Engagements.
  organization has set to police transactional risks.

July 2018 - June 2021

Senior Information Security Consultant Univate Solutions

- Iso27001 Auditor, managing clients from middle east and Canada.
- Suggest and execute IT technologies, strategies, and policies to guard customer's information assets.
- Implement security risk analysis for current and new systems to find system weaknesses or disclosures.
- Recommend solutions for explaining risks and reducing exposure areas.
- Prepare security program plans and execute IT controls, processes, audit tools, interfaces, and utilities for authentication.
- Perform as chief for audits and security aspects.
- Support and provide consultancy for audit compliance actions.
- Implement periodic, on-demand project audits plus vulnerability analysis.
- Determine compliance through user accounts, application usage, system file and outside scans.

August 2015 - June 2018

Information Security Consultant B2C Engage Technologies

Gained operational experience in a Security Operations Centre (SOC), monitoring, and analyzing security events to detect and respond to potential threats.
Assisted in the management of Incident Response SIEM tools, contributing to the swift and effective resolution of security incidents.
Conducted regular reviews of security policies, protocols, and technologies to align with industry standards and compliance requirements.
Actively participated in threat modeling and risk assessment exercises, identifying potential weaknesses, and recommending appropriate controls.
Collaborated with cross-functional teams to ensure a cohesive security strategy and smooth incident response procedures.
Communicated effectively with team members, stakeholders, and leadership to convey security-related information and ensure a shared understanding of security priorities.

June 2012 - July 2015

Cyber Security Specialist Suvenbits Technologies

- Helped the organizations to achieve ISO 9001, ISO 27001, ISO 22301, HIPAA compliance and CMM Level 3and 5 for various organizations.
- Assisted in Setting up and operationalization of PMO by defining standards, procedures, roles and responsibilities, metrics, governance.
  / Controls
- Network Tools: Nmap, Wire Shark, Nessus, Qualys Guard
- Port/Vulnerability Scanning: Nmap/Nmap Scripting Engine (NSE), NetCat, Nessus
- Planning, Conducting, and reporting Vulnerability and risk assessmentof applications.

Risk associated with vulnerability explained to the project team for
Conducted in-depth application security assessments to identify potential vulnerabilities and recommend remediation strategies, resulting in

improved application security.
Assisted in vulnerability management efforts, including vulnerability scanning, patch management, and the timely resolution of identified vulnerabilities.
Contributed to threat assessments by monitoring security events, conducting analysis using SIEM tools, and collaborating with the incident response team to mitigate threats promptly.
Actively participated in multi-discipline security engineering tasks, ensuring the security of critical assets and infrastructure.
Maintained a strong knowledge of security principles, protocols, and technologies, implementing best practices to protect sensitive data.
Ensured compliance with relevant regulations and compliance requirements, including industry standards and data protection laws.
Collaborated with cross-functional teams to perform threat modeling, risk assessments, and vulnerability management, fostering an initiative-taking security approach ensure the appropriate level of protection and adherence to thegoals of the overall information security strategy.

September 2010 - March 2012

Application Security specialist Capgemini Private Limited

- Perform security tests on cloud networks, web-based applications, mobile-applications.
- Design these tests and tools to try to break into security-protected applications and networks to probe for vulnerabilities!
- Keep up with the latest methods for ethical hacking and testing and are always evaluating new penetration testing tools!
- Use testing methods to pinpoint ways that attackers could exploit weaknesses in security systems.
- Conducting network and system security audits, which evaluate how well an organization's system conforms to a set of established criteria.

November 2009 - April 2010

Infrastructure management Analyst Xerox Services

- Good knowledge of Client Management & Direct connect.
- Windows/Linux/Mac OS Platform troubleshooting knowledge will be an added advantage.
- Ability to operate in a dynamic, evolving environment.
- Ability to interface with vendors to diagnose and troubleshoot problems.
- Review the reports based on the frequency of the outage.
- Was serving close to three thousand clients.
- Global Network operation center

.

EDUCATION

May 2004

Bachelor's | Information Technology