

ANUPAM KUMAR

Information Security Manager

Email: anupmkmr@outlook.com; Mobile: +85267205096

A seasoned Information Security Officer with 4+ years of experience in risk management, governance, and operational resilience, specializing in cybersecurity technologies such as SIEM, SOAR, and XDR. Proven track record in maintaining robust security postures, ensuring compliance with international security standards (ISO 27001, NIST), and advising on security strategies for complex business environments. Adept at collaborating with cross-functional teams to align with corporate security standards and regulatory requirements while addressing security threats and risks.

Skills

- **Information Security & Risk Management:** Security Governance, Security Risk Assessment, Risk Register Management, Incident Response, Cyber Crisis Management Plan
- **Security Standards & Compliance:** ISO 27001, NIST, Regulatory Compliance.
- **Security Technologies:** SIEM, SOAR, Privileged Access Management, WAF, Anti-DDoS, Data Leakage Prevention, XDR, Anti-APT, DAM, Deception Technologies.
- **Security Assurance:** Vendor Security Assurance, Penetration Testing, Vulnerability Management, Security Audits
- **Collaboration & Communication:** Strong advisory and communication skills for aligning business teams with security standards

Professional Experience

Bank Of India- Information Security Manager

Oct 2020-Present

Security Governance & Risk Management:

- Played a key role in development and implementation of security risk management strategies, ensuring that all technology solutions comply with security standards and regulations, including ISO 27001 and NIST.
- Conduct comprehensive security risk assessments, identify vulnerabilities, and create strategies to mitigate potential threats to maintain the organization's security posture.
- Maintain and regularly update the security risk register, ensuring the communication of identified risks to key stakeholders.

Cloud Security:

- Played a key role in securing cloud environments by designing and implementing security controls across platforms like GCP and Azure.
- Successfully deployed and configured an OpenShift cluster on Nutanix infrastructure to support IBM UAX, ensuring secure integration, optimal performance, and compliance
- Provided ongoing security guidance to development teams on vulnerabilities, secure deployment practices, and conducting vulnerability assessments.

NG-SOC Design & Integration:

- Led the design and implementation of a comprehensive Next-Generation Security Operations Center (NG-SOC), integrating advanced security technologies (EDR, SIEM, SOAR, XDR Connect, Anti-APT) for seamless threat detection, incident response, and security orchestration, while developing business continuity and disaster recovery procedures.
- Ensured optimal performance of SIEM, SOAR, and EDR platforms, automating incident response workflows with SOAR playbooks to improve detection, response efficiency, and change management processes.

Security Advisory & Incident Management:

- Provided professional security advice to project teams, business units, and senior management, ensuring all solutions align with corporate security standards and best practices.
- Played a key role in security incident management efforts by working with first responders, identifying, containing, and resolving security incidents in a timely manner.
- Collaborated with external penetration testing providers to identify gaps in existing security frameworks and improve risk mitigation strategies.
- Collaborated with cross-functional teams to align cybersecurity operations, leveraging emerging threat intelligence and MITRE frameworks to develop security use cases and strengthen the organization's security posture and compliance.

Vendor & Compliance Assurance:

- Managed the vendor security assurance process, reviewing third-party solutions to ensure they meet the organization's security and compliance requirements.
- Assisted in preparing for internal and external security audits, ensuring all security controls are adequately implemented and addressing any findings or gaps identified during audits.

Security Documentation & Reporting:

- Maintained and updated security policies and operational processes to enhance security controls and ensure continuous improvement in the organization's security posture.
- Prepared detailed management reports and presentations for the Chief Security Officer and executive teams, providing insights on risk management, security incidents, and mitigation strategies.
- Reviewed Cyber Crisis Management Plan (CCMP) and Cyber Security Policy Framework (CSPF) to ensure alignment with current cybersecurity trends and regulatory advisories and guidelines.

Educational Qualifications & Certifications

Education

- **Master of Technology - Digital Communication**
Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, India | March 2019

Certifications

- **Arcon PAM Administrator** | Arcon | December 2021
- **Certified Ethical Hacker (CEH V11)** | EC-Council | April 2022
- **ISO 27001 Lead Auditor (ISMS)** | TUV SUD | September 2023
- **CompTIA Security+** | CompTIA | April 2024
- **Certified in Cybersecurity (CC)** | ISC2 | July 2024
- **CompTIA Security Analyst Professional (Security+ and CySA+)** | CompTIA | Dec 2024
- **Certified Information Systems Security Professional (CISSP)** | ISC2 | In Progress

Other Information

- **Visa Status:** Eligible to work in Hong Kong under the General Employment Policy
- **Language:** English (Fluent), Chinese (Learning)
- **Nationality:** Indian