RAHUL B. KATWE

Email: rahulk919@gmail.com
Web: www.linkedin.com/in/rahulkatwe
Phone: +91-9420880140

Bachelor of Engineering, Computer Science with 69.06% from Mumbai University.

DYNAMIC PROFESSIONAL WITH 5 Years & 6 Months OF EXPERIENCE
(Currently associated with UBS as an IT Risk and Controls Specialist)
Business-Support • Delivery • Hard-working • Confident • Proactive

Career Overview:

Energetic, value-driven, and result-oriented Information Security and Risk Management professional with over five years of experience in managing information security of multi-national Banks. Extensive experience in IT Audit, Third Party Risk Management, business continuity management. Skilled in prioritizing tasks independently and proficient in identifying gaps in processes or systems.

Objective:

To work in a security-focused environment where I can use acquired knowledge of managing risks and develop expertise as a security architect in designing, building, and maintaining a secure business environment while at the same time striking a balance between security and functionality through a cost-effective approach.

Achievements:

- Fast-Track Promotion as on 1st Jan 2018 to Senior Analyst in Deutsche Bank.
- Achieved outstanding performance award in UBS Bank.
- ISO 27001:2013 LA completed.
- ICSI CNSS course completed.

Work Experience:

1. UBS Business Solutions (India) Private Limited

Role: IT Risk and Control Specialist
Period: April 2019 – Present
Location: Pune, MH

Summary: Manage and restrict sensitive data disclosure to offshoring initiatives within UBS.

- Assist with the planning of information technology and data privacy assessments by understanding organization objectives, structure, policies, processes, internal controls, and regulatory requirements.
- Coordinate with a global team that manages outsourcing initiatives based on limiting access to restricted sensitive client identifying data.
- Understand and assess offshoring of access rights by identifying scope, access rights functionality, business objectives and data privacy risk areas associated with the software component.

- Understand legal and business requirements for cross-border data transfer within UBS.
- Compile and complete assessment results by checking legal and business restrictions on cross-border data transfer which may be disclosed by the application in assessment scope. Legal and business conditions are defined in a Client Disclosure Table which highlights region/country restrictions for all active UBS entities. Legal requirements are based on country specific data privacy law and principles such as GDPR, Data Protection Act etc.
- Verify evidence shared by the software component manager confirming no sensitive or client identifying data disclosure by the software component.
- Conduct initiation and closure meetings with the business requester, software component managers, and technical SMEs throughout the assessment phase and develop and maintain business relationships with stakeholders and control functions involved in the access rights assessment process.
- Manage entire workflow over service management tools such as ServiceNow and JIRA.
- Analyze and advise on all data protection queries from different members of the Business teams, providing information and issue recommendations to the Business teams.
- Work with the legal team in the review of any legal contracts and advise where necessary on data sharing arrangements and data processing agreements.
- Engaged in continuous knowledge sharing and operational process improvement for Access Rights Assessment.

2. Deutsche Bank Group (DBOI)

Role: Information Security Analyst
Period: Feb 2016 – Mar 2019
Location: Pune, MH

➢ Process 1: Application Risk Assessment

Summary: Application-level Risk assessment for all bank owned applications to fulfill the compliance part as well as a focused process to ensure the bank's information security.

- Understand and analyze business setting from an information security perspective.
- Ensure the effectiveness of Application compliance with Deutsche Bank's IT Security Policies.
- Interact closely with the business, IT solution owners to discuss about controls and its remediation plans.
- Responsible to perform end to end Information Security Risk Assessment.
- Assisting business in completing their open risk areas.
- Support the business during Audits and with Audit resolution as it relates to issues that address information security in their areas processes and projects.
- Information Security Internal Audits: Conduct internal information security audits as per ISO 27001:2013, company policies, and client security requirements. Understand the information security requirements as signed in the contractual agreement with the client and prepare a checklist in line with the security requirements to perform an internal audit to ensure that the location is compliant to ISO 27001 standard.
- Ensures that adequate and effective security processes and controls are followed and aligned by establishing appropriate assessments, managing and tracking risk mitigation and remediation activities.
- Conduct risk assessments for the enterprise by reviewing physical, technical, and administrative controls based on NIST 800-53 Risk Management Framework.

➢ Process 2: Third Party Risk Assessment

Summary: Perform Inherent Risk Assessment based on third-party services, questionnaire-based risk assessment for high-risk vendors, Findings Management and part time engagement management.

- Understand the client's information security governance and operating model for assessing vendor/third-party risk.
- Identify key stakeholders for the assessment not limited to the business team, procurement, vendor and client POC, legal POC, and senior management.
- On-board new vendor to client's third-party vendor risk management program and maintain inventory of existing vendors by categorizing them as per their services and risk rating.
- Perform an inherent risk assessment with a client relationship manager to understand third-party size, their services, client data access, client system access and SLA requirements under the engagement.
- Conduct a full questionnaire-based risk assessment with the third-party based on the inherent risk rating to understand third-party security posture and design effectiveness of the vendor's security program.
- Review vendor's response to the assessment questionnaire and verify third-party policies, procedures, and independent audit reports such as SOC 2, HITRUST, and PCI DSS Compliance Report, etc.
- Review network and application vulnerability assessment, penetration test and static code analysis reports shared by the vendor and identify gaps for remediation.
- Coordinate with the client's internal network security, application security, data privacy and legal teams for complex cases.
- Maintain strong client focus by building strong relationships with senior security leadership, internal security teams and business personnel.
- Coordinate with the third-party to remediate findings identified during the assessment and monitor issue remediation and risk treatment performed by the third party.
- Assist the client in third-party termination at the end of vendor lifecycle.
- Manage entire workflow on vendor risk management platforms such as ServiceNow, Process Unity and RSA Archer.
- Play a key role in the development of less experienced staff through mentoring, training and advising team members and help them understand information security concepts.

Education:

- **Bachelors of Engineering (B.E)**

Institute - Yadavrao Tasgaonkar Institute of Engineering & Technology (YTIET)
Major - Computer Science
University - University of Mumbai
Completed my graduation in Computer Engineering with Cloud computing as an area of interest.

- **H.S.C and S.S.C**

Board - Maharashtra State Board of Secondary and Higher Secondary Education
10+2 in Computer Science.