Ravinder Kumar

CISA | Cybersecurity Risk & GRC Analyst | Regulatory Audit, Risk & Compliance
yadavravinder833@gmail.com | +91-9318406405 | Gurugram, Haryana, India | linkedin.com/in/ravii10

Profile Summary

- CISA-certified cybersecurity risk and GRC professional with experience assessing information security risk management activities, evaluating control effectiveness, and reporting risk to leadership across SEBI-regulated financial market infrastructure entities.
- Hands-on experience in third-party / vendor risk management and risk-exception & treatment lifecycle governance, including RCA, remediation tracking, and risk-based reporting for regulatory and executive audiences; reviews BCP/DR plans as part of cyber resilience oversight.
- Working knowledge of RBI Cybersecurity Framework, NIST CSF, ISO 27001, and PCI DSS alongside deep SEBI CSCRF expertise, enabling cross-framework risk and audit alignment; monitors regulatory developments and translates them into audit requirements.
- SOC background in SIEM, EDR/XDR, DLP, and vulnerability management adds technical depth to risk oversight that most GRC-only profiles lack. CySA+, CEH, Security+, AZ-500 certified.

Core Competencies

- Cybersecurity Risk Governance & Oversight
- Third-Party / Vendor Risk Management (TPRM)
- Risk Exception & Treatment Tracking
- Cyber Resilience (BCP/DR Review)
- SEBI CSCRF Compliance, Audit & Enforcement
- Multi-Framework GRC: RBI CSF, NIST CSF, ISO 27001, PCI DSS
- Regulatory Inspections & Control Assessments
- Risk Assessment & Root Cause Analysis (RCA)
- Executive & Committee Risk Reporting
- Incident Response Governance
- Vulnerability Management Oversight
- Data Protection (DPDP Act, ISO 27001)

Technical Skills

- **Cybersecurity Audit & Risk Frameworks:** CISA, SEBI CSCRF, RBI Cybersecurity Framework, NIST CSF, ISO 27001, PCI DSS, DPDP Act 2023
- **Security Operations:** SIEM (Splunk, ELK Stack), EDR/XDR, DLP, SOC Operations, Incident Response
- **Assessment Tools:** OpenVAS, OWASP ZAP, Vulnerability Assessment
- **Cloud & Infrastructure:** Azure, Firewall & Network Security, Linux
- **Scripting:** PowerShell, Python

Organisational Experience

Securities & Exchange Board of India (SEBI), Mumbai Since Nov'24
Cyber Security Analyst (YP)

- Support risk management oversight of cybersecurity risk by driving regulatory compliance audits across SEBI-regulated Market Infrastructure Institutions (NSE, BSE), verifying adherence to the Cyber Security and Cyber Resilience Framework (CSCRF) and reporting compliance gaps to leadership.
- Assess information security risk management activities by reviewing and validating third-party cybersecurity audit reports submitted by regulated entities, ensuring findings meet regulatory quality and completeness standards before sign-off.
- Identify potential risks and control gaps by leading cybersecurity inspections and control assessments, coordinating remediation/risk-treatment timelines with regulated entities, and advising them on control implementation and audit readiness for CSCRF and related frameworks.
- Manage end-to-end incident and risk-exception lifecycle governance, including RCA documentation and risk-based reporting to support executive and regulatory audiences; designed audit-ready incident response playbooks and SOPs to standardize reporting.
- Support third-party risk oversight by evaluating audit firms and security vendors for CSCRF engagements, assessing scope, methodology, and finding quality; support cyber resilience oversight by reviewing BCP/DR plans, verifying recovery time and recovery point objectives.
- Monitor evolving laws, rules, and regulatory guidance related to cybersecurity risk to keep audit and reporting practices current.

Code Caters IT Solutions, Gurugram Jun'23 – Nov'24
Associate

- Monitored enterprise systems and network logs in a SOC environment using Splunk and ELK Stack, detecting and analyzing 15+ security incidents per week; investigated alerts using EDR/XDR solutions to support triage, containment, and remediation.
- Assisted in Data Loss Prevention (DLP) monitoring and policy enforcement, preventing data exfiltration and ensuring compliance with organizational security standards.
- Implemented and administered Mobile Device Management (MDM) across 300+ endpoints using Microsoft Intune and ManageEngine, enforcing device compliance, remote wipe, and encryption standards.
- Performed vulnerability assessments using OpenVAS and web application testing with OWASP ZAP to identify and report security risks; supported incident response and RCA, preparing incident summaries and assisting in developing incident response playbooks.

Education

Bachelor of Engineering (CSE Hons.), Information Security 2020 – 2024
Chandigarh University

Certifications

CISA (Certified Info. Systems Auditor) | Azure AZ-500 | CompTIA CySA+ | Certified Ethical Hacker (CEH) | CompTIA Security+