POONAWALLA FINCORP

IT GRC Job Description

IT GRC (Governance, Risk, and Compliance) team is responsible for ensuring that the organization's IT operations align with governance frameworks, manage IT risks, and comply with legal, regulatory, and industry standards. Their roles and responsibilities often include:

Roles & Responsibilities: -

Governance Responsibilities

- Overseeing the review and management of IT documentation, ensuring accuracy, completeness, and compliance with internal policies, regulatory mandates, and industry standards.
- Spearheading the design and implementation of robust IT GRC policies and procedures to ensure regulatory compliance and mitigate risk factors within the banking technology sector.
- Establishing and maintaining effective governance structures to monitor and enforce IT GRC controls, safeguarding critical assets and ensuring business continuity.
- Ensuring policies and framework for crisis management and business continuity planning, ensuring IT systems' resilience in the face of disruptions and disasters.

Compliance Responsibilities

- Conducting PCI-DSS & DPSC GAP Assessment & Remediation for the PFL.
- Achieving successful compliance certifications (e.g., ISO 27001) through rigorous audit preparation and documentation.
- Orchestrating Regulatory Information Technology compliance requirements for PFL, meticulously overseeing the timely filing of various regulatory reports to RBI and other governing bodies.
- Leading and coordinating RBI (CSITE) and other regulatory audits for the technology department, orchestrating comprehensive compliance assessments and driving resolution of identified issues.
- Submission of IT Compliance reporting on a weekly/monthly basis which includes Antivirus Status, Patch Status, Hard disk encryption status.
- Single point of contact for all Information Technology compliance related requirements.
- Analyze the circulars published by regulatory bodies like Reserve Bank of India, NPCI, IRDA, and ensuring compliance to the same.
- Test design and implementation for the controls and discussed the gaps found during the audits.
- Leading RBI (CSITE) and RBI SSM audits for technology department.
- Track various audit observations till closure.
- Managing user access management for IT applications with PFL

POONAWALLA FINCORP

Collaboration and Communication Responsibilities

- Collaborating with legal and regulatory affairs teams to interpret and address new regulatory requirements affecting IT operations.
- Spearheading the facilitation of Third-Party Audits for IT functions, ensuring thorough assessment of compliance with internal policies and external regulations, and driving continuous improvement initiatives based on audit findings.
- Collaborating with cross-functional teams to develop and implement robust governance frameworks, policies, and procedures, fostering a culture of compliance and risk awareness across the organization.
- Support internal, external, and regulatory IT audits including SOX, operational, financial audits, and other risk-based engagements. (RBI, CSITE SEBI, IRDAI, UIDAI, ITGC, SOX)

Risk Management

- Identifying risk and recommending mitigating controls to maintain and manage risks.
- Coordinating with InfoSec to perform the Risk Assessment on identifying the critical applications and to include the same in the PFL's BCP policy.
- Monitor and report on key risk indicators (KRIs) and risk appetite.

Continuous Improvement

- Preparation for getting recognition for outstanding contributions to CSITE Audit within the organization.
- Conducting thorough analysis of advisories and circulars issued by regulatory authorities such as RBI, NPCI, IRDA, and UIDAI, ensuring meticulous alignment with regulatory guidelines and standards.
- Proactively identifying emerging regulatory trends and requirements and implementing proactive measures to ensure continuous compliance and mitigate associated risks.
- Implementing ITIL processes: Incident Management, Change Management, Release & Deployment Management, and IT Service Continuity Management.
- Establishing effective metrics and managing escalations to ensure service quality.
- Analyzing reports, presenting insights to Management, and driving continuous service improvements.
- Ensuring strict adherence to processes and guidelines for seamless service delivery.
- Leading initiatives to enhance IT GRC awareness, fostering a culture of compliance and accountability across the organization.
- Driving continuous improvement efforts to optimize IT GRC processes and frameworks, leveraging industry best practices and emerging technologies to stay ahead of evolving regulatory requirement
- Collaborating with cross-functional teams to conduct comprehensive risk assessments and develop tailored mitigation strategies to address emerging threats and vulnerabilities.
- IT Security Architecture Review & Advisory DDoS,
- Vulnerability Assessment Penetration Testing
- Preparing Quarterly presentation for IT Steering Committee, IT Strategy Committee, etc. Making sure that Audits are performed regularly for; Inventory Management, Change Management, Patch Management, User Access Management, Incident Management, Vendor Risk Management, Capacity Management, BCP, Disaster Recovery, Cyber Security.
- Performing Critical Application Audits and Critical Vendor Audits based on the Risk Assessment.

POONAWALLA FINCORP

Education	MCA/MBA/MTech- Computer Science/IT
Experience	15-20 years
Certifications	ITIL, PMP, TOGAF, COBIT, DevOps, etc.
Team Size managed	20

Below are a few listed activities that IT GRC would perform.

CAB - Change Advisory Board	IT Steering Meeting -- Project updates, budget details
User Access Review	IT Security Compliance Review
Email Access Review	SOP Review and its closure
Generic email access review	Vendor Self-Assessment
Distribution List Review	IT Risk Register Responses
Privilege Access User Review	RBI Compliance - Data as requested
VPN Access Review	GAP Assessment -- Closure of identified gaps with Infosec, IT
VAPT - Review and Closure	Agreement Review -- Agreement and related information
BCP - DR Setup and Drill	Documentation -- As and when required for documentation
RBI Inspection	Vendor Onboarding Process -- Periodic review
IS Audit (RBI, MD, NBFC)	Maintenance of Master Policy Repository
Policy / Procedure Review	New RBI Master direction implementation
KRI - ORM Team	PFL _ RBI _ Guideline for Secure Application Design
RAF - Review and Closure	Master Repository at Application Level, Database Level, API Level etc..
IT Strategy Meeting -- Project updates, budget details, Infosec slides	ITGC and IFC Audit
Internal Vendor Audit	Application-Level Reports SOC2, VAPT, BCP-DR and ISO 27001
DPDP Act Implementation	Annual Report