**[](https://www.smartsheet.com/try-it?trp=11223&utm_source=integrated+content&utm_campaign=/content/pmo-templates&utm_medium=PMO+Standard+Operating+Procedure+(SOP)+doc+11223&lpa=PMO+Standard+Operating+Procedure+(SOP)+doc+11223&lx=PFpZZjisDNTS-Ddigi3MyABAgeTPLDIL8TQRu558b7w)**

**Governance, Risk & Compliance**

**For India IT Industry  
(GRC) TEMPLATE**

<COMPANY NAME>

Street Address

City, State and Zip

Version 0.0.0

00/00/0000

# VERSION HISTORY

| VERSION NO. |  | CURRENT VERSION DATE |  |
| --- | --- | --- | --- |
| **EFFECTIVE DATE** |  | **EXPIRATION DATE** |  |
| **RESPONSIBLE PERSON** |  | **SIGNATURE** |  |
| **WRITER** |  | **APPROVAL** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| <COMPANY NAME>**. <GRC (Governance, Risk, and Compliance)>** | | | | | |
|
|
|  | | | | | |
|  | **Document Management Information** | | | | |
|  | | | | | |
|  | **Document Publication History** | | | | |
| All revisions made to this document must be listed in chronological order, with the most recent revision at the top | | | | |
|  | | | | | |
|  | **Version #** | **Date** | **Author(s)** | **Reviewer and Approver** | **Remarks** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  | | | | | |
|  | | | | | |
|  | **Document Owner: PM** | | | | |
|  | | | | | |
|  | **Document Classification: Internal**/Public/Confidential/Restricted | | | | |
|  | | | | | |
|

# Table of Contents

1. Introduction

2. Definitions

2.1 Governance

2.2 Risk Management

2.3 Compliance

3. Importance of GRC

4. Drivers for GRC Implementation

5. How GRC Works

5.1 Key Stakeholders

5.2 GRC Framework

5.3 GRC Maturity

6. GRC Capability Model

6.1 Learn

6.2 Align

6.3 Perform

6.4 Review

7. Common GRC Tools

8. Challenges in GRC Implementation

9. Steps to Implement an Effective GRC Strategy

10. Role of IT in GRC (India IT Context)

# 1. Introduction

GRC (Governance, Risk, and Compliance) is a unified framework that enables organizations to align IT and business objectives, manage risk, and adhere to regulatory and policy requirements. For the Indian IT industry, GRC plays a crucial role in meeting global client expectations, protecting sensitive data, and ensuring compliance with Indian regulations such as the IT Act 2000, CERT-In guidelines, and the Digital Personal Data Protection Act (DPDPA) 2023.

# 2. Definitions

## 2.1 Governance

Governance is about defining policies, procedures, and controls to guide decision-making. In the Indian IT sector, this includes data protection frameworks, ethical outsourcing practices, and transparent reporting to stakeholders.

## 2.2 Risk Management

Risk management involves identifying and mitigating potential risks such as cybersecurity threats, service disruptions, and data breaches. IT service providers in India must address risks from ransomware, phishing, and supply chain vulnerabilities while ensuring SLAs are met.

## 2.3 Compliance

Compliance ensures adherence to laws and standards such as ISO 27001, SOC 2, GDPR (for EU clients), and DPDPA 2023 (for Indian data subjects). Non-compliance can lead to legal penalties, reputational damage, and loss of client trust.

# 3. Importance of GRC

For Indian IT service companies, GRC is critical to maintaining global credibility, winning outsourcing contracts, and safeguarding intellectual property. It helps create a resilient, risk-aware organization capable of handling rapid changes in regulatory environments.

# 4. Drivers for GRC Implementation

Key drivers in India include:  
- Strict enforcement of data protection laws (DPDPA 2023)  
- Rising cyber threats and ransomware attacks  
- Client requirements for compliance with international standards  
- Demand for business continuity and disaster recovery readiness  
- Growing cost of regulatory penalties and data breaches

# 5. How GRC Works

## 5.1 Key Stakeholders

CISOs, CIOs, compliance officers, HR, and IT security teams play crucial roles in GRC implementation.

## 5.2 GRC Framework

Indian IT organizations adopt frameworks such as COBIT, ISO 31000, and NIST to structure governance and risk programs.

## 5.3 GRC Maturity

Mature GRC practices include proactive monitoring, real-time risk assessments, and continuous compliance reporting.

# 6. GRC Capability Model

Learn – Understand risks and compliance requirements (DPDPA, GDPR, etc.)

Align – Map IT processes with organizational goals and client obligations

Perform – Execute security controls, audits, and awareness programs

Review – Continuously monitor compliance posture and improve

# 7. Common GRC Tools

Indian IT companies use tools like Archer GRC, ServiceNow GRC, AWS Audit Manager, and SIEM platforms like Splunk or ELK stack.

# 8. Challenges in GRC Implementation

Challenges include lack of skilled cybersecurity professionals, fragmented compliance requirements across jurisdictions, and difficulty in automating compliance reporting.

# 9. Steps to Implement an Effective GRC Strategy

1. Define clear business and compliance goals  
2. Assess existing processes and gaps  
3. Obtain leadership buy-in  
4. Implement security automation and monitoring  
5. Train employees on data security and compliance  
6. Perform regular internal audits

# 10. Role of IT in GRC (India IT Context)

IT plays a central role in implementing GRC by enforcing least-privilege access, securing data centers and cloud workloads, maintaining audit trails, and integrating compliance automation tools with DevOps workflows.

For the Indian IT industry, GRC is no longer optional but a strategic necessity. Organizations must adopt a holistic, technology-driven GRC approach to stay competitive, protect client data, and remain compliant with evolving regulations.

# GRC Capability Model (Table)

|  |  |
| --- | --- |
| **Capability** | **Description** |
| Learn | Understand regulatory requirements (DPDPA 2023, GDPR), business objectives, and risks. |
| Align | Align IT operations with compliance frameworks and client expectations. |
| Perform | Implement security controls, monitoring, employee training, and audits. |
| Review | Continuously evaluate effectiveness, improve controls, and adapt to new threats. |