Vakrangee
सशक्त परिवर्तन

GOVERNANCE, RISK AND COMPLIANCE POLICY (GRC)

Contents

1. Introduction

This document is the property of Vakrangee Limited and is for use only by Vakrangee Limited or any of its group Companies. It must not be copied, disclosed, circulated or referred to in correspondence with external parties or discussed with any other party other than for any regulatory requirements without prior written consent from the Management and the Anti- Fraud Committee.

2. Governance

Ensuring that organizational activities, like managing IT operations, are aligned in a way that supports the organization's business goals.

We have established a Corporate Security and Compliance Team (CSC) made up of key personnel whose responsibility is to identify areas of security and compliance concern across the organization and act as the first line of defence in enhancing the appropriate security and compliance posture. This team reports to the Chief Technology Officer.

The team comprises the workforce who are knowledgeable in legal cross-regulation, policy, products, and IT, and are interested in ensuring five of the trust principles—confidentiality, integrity, availability, privacy, and security—with regard to data protection by law, compliance, and standards across the organization. The Chief Technology Officer has assigned the responsibilities and authority to Data Protection Officer for overseeing and maintaining information security and compliance as per the standard and industry best practices.

The governance of these programs is performed by the Corporate Security and Compliance Committee, consisting of executives and other department heads across the organization.

3. Risk

Making sure that any risk (or opportunity) associated with organizational activities is identified and addressed in a way that supports the organization's business goals. In the IT context, this means having a comprehensive IT risk management process that rolls into an organization's enterprise risk management function.

We have established and implemented robust Risk Management Procedure and Process in place and conduct periodic risk assessments for the organization using the baseline methodology based on ISO 27001 standard framework with cross-reference with ISO 9001, PCI DSS and industry best practices.

We are not willing to accept any risk that might damage customer trust. In addition, any risks that threaten to make us non-compliant to regulations and standard. Risk Treatment Plan involves prioritizing, evaluating, and implementing appropriate controls as per the risk computation.

4. Compliance

Making sure that organizational activities are operated in a way that meets the laws and regulatory requirements impacting the systems. In the IT context, this means making sure that IT system, and the data contained in those systems, are used and secured properly.

We have established a formal Compliance Policy and Procedure which addresses aspects of compliance required to be adhered to and fulfilled with respect to our Information Security Policies. This policy also addresses the legal and compliance requirements pertaining to relevant statutory legislation, and contractual and regulatory obligations which we are supposed to adhere to in order to protect its documents, records, and assets, thereby preventing the misuse of information processing facilities. Such efforts would help us establish, maintain, and sustain the desired information security and privacy posture aligned with our strategic business plan, based on the best practices, standards, and principles.

We are committed to and conducts its business activities lawfully and in a manner that is consistent with its compliance obligations.

We have been identifying all relevant regulatory and legislative requirements in lien of its contractual requirements and organization's operational requirements and defining, documenting, and updating it on a regular basis.

All records, as mandated by statutory/legal/regulatory authorities in India or of foreign origin, for which we are responsible for compliance, shall be protected from intentional or unintentional damage through natural causes.

The retention limit of statutory records shall be as mandated by the applicable legislation. However, for business records/documents, the business group heads and or HODs shall determine the retention limit with justification.

We shall always seek to protect the privacy of the personal information of its customers, employees, and third parties with whom We have signed the third-party agreement. Divulging of facts shall be done only in keeping with statutory/contractual/regulatory/legal requirements. Such information shall always be protected from getting misused, leaked, or falsified or traded with any interested party knowingly or unknowingly.

Where logs are required to be maintained as per contractual/regulatory/statutory/legal requirement, these shall be maintained for a specified duration.

Data or records that are no longer required for business, legal, and/or regulatory purpose shall be disposed of securely.

Legal restrictions on the use of assets in respect of which there are IPRs (such as copyright, software license, trademarks, design rights, and others) shall be complied with.

Intellectual Property Rights of software programs, documentation and other information generated by or provided by our users, consultants, and contractors for the benefit of the organization, shall be the property of the organization.

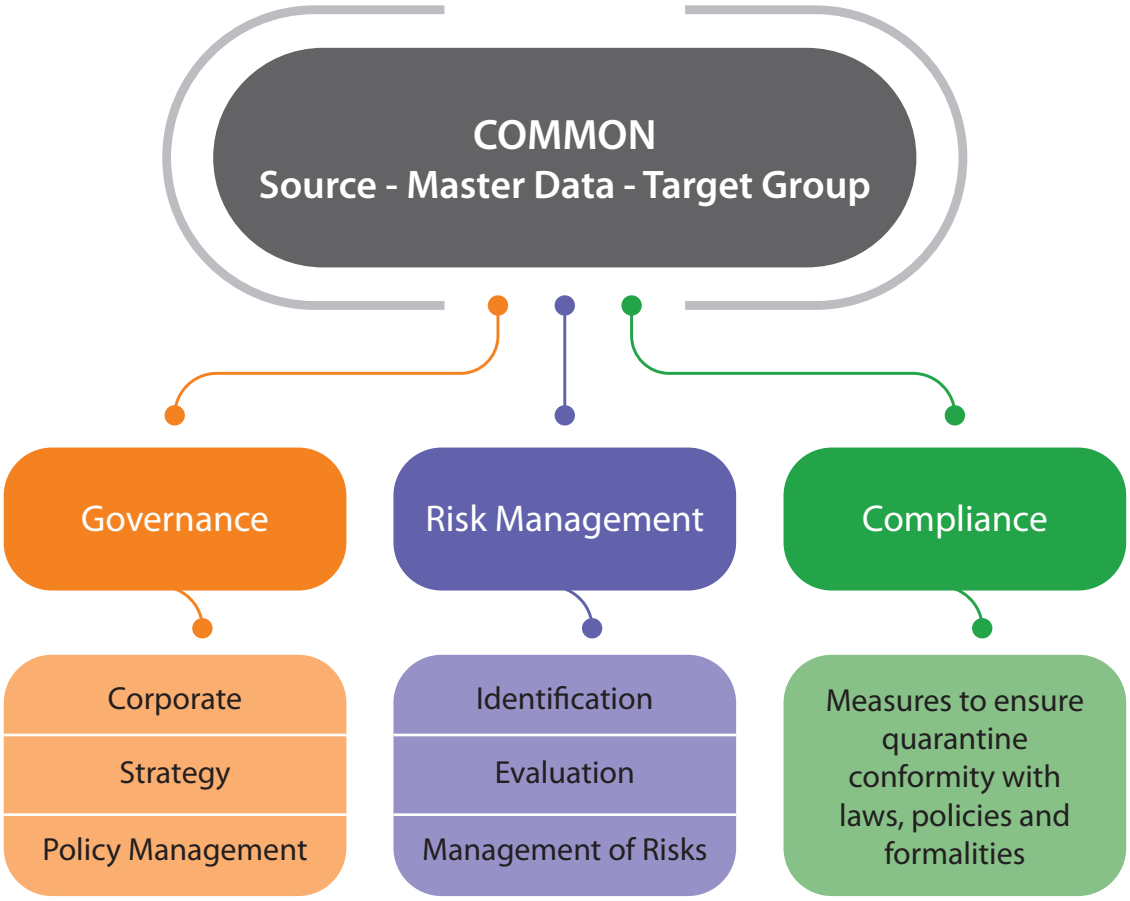
Intellectual Property Rights shall be included in all contracts.

Relevant statutory, regulatory, and contractual requirements for our information assets shall be defined explicitly. Such requirements shall include, but are not limited to:

- Information Technology Laws (IT Act 2008/2011 Amended) (GOI)
- Software Licensing Requirements
- Intellectual Property Rights (IPR) Laws
- Labor and General Employment Laws
- Health and Safety Laws
- Environmental Laws

As part of the information security audits by independent consultants or body, the appropriate confidentiality and non-disclosure agreements shall be signed with them. And any access granted to the external shall be restricted immediately after completion of the audit.

Compliance requirements are used to enforce a minimum level of security and privacy within the organization. These are by no means a "finish line" for security and privacy.



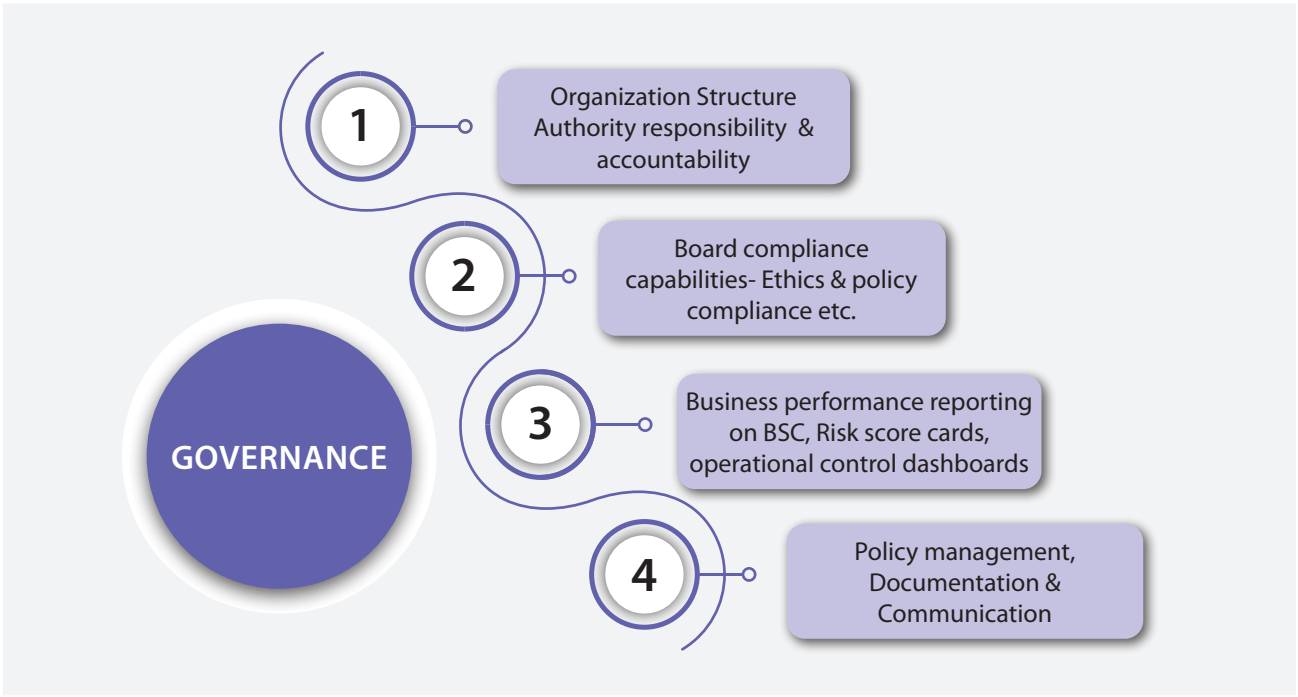
5. IT Governance, Risk and Compliance Policy Scope

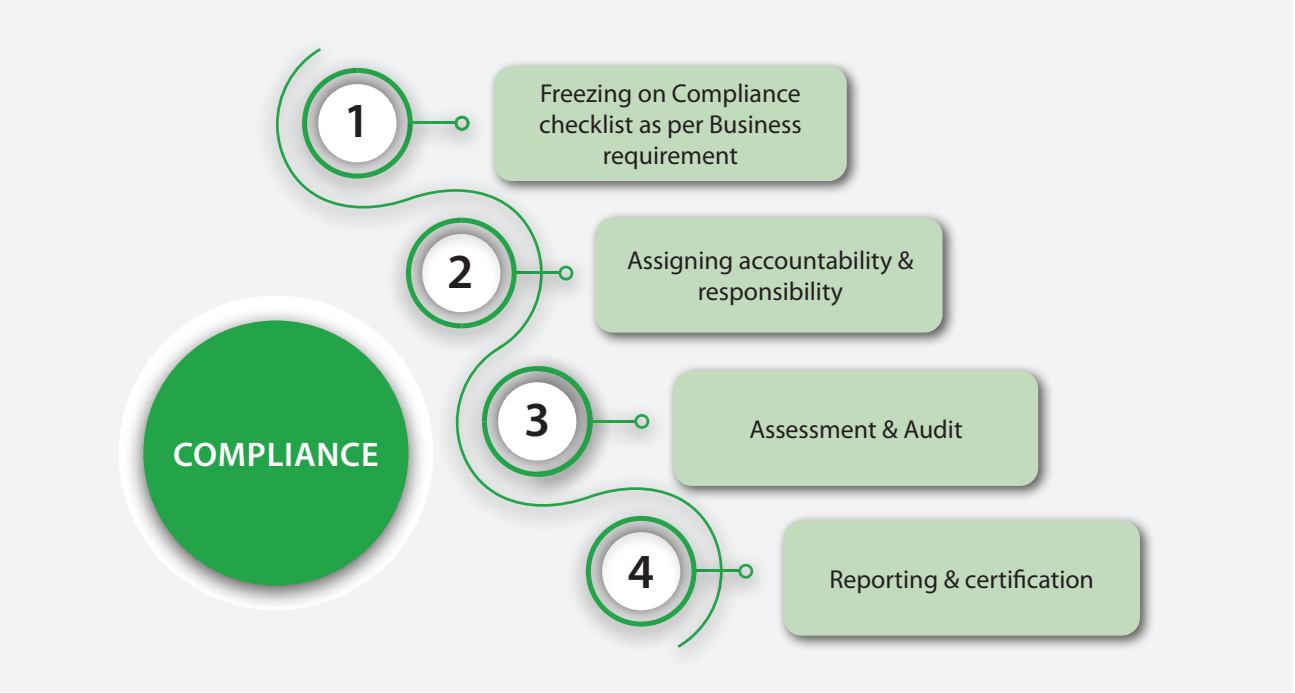
This policy applies to all activities of the organization related to Information Technology

6. IT Governance, Risk and Compliance Policy Principles

- Govern us to meet the expectations of Shareholders and stakeholders, in the outcomes achieve through open and transparent communication
- Promote a performance culture where we focus on its objectives and accept responsibility for recognizing, communicating and managing the uncertainty (opportunities and threats) to these objectives;
- Promote an organizational focus on IT Governance, Risk and Compliance to support the business in effectively integrating governance, risk and compliance into business decision making and business processes.
- Execute timely decisions which create and protect business value having considered the best available information and taking account of uncertainty
- Understand and comply with our legal, regulatory and other obligations
- Understand those risks that threaten the ongoing operation of our organization and have in place strategies to minimize business disruption.

7. IT Governance, Risk and Compliance Policy Objectives





8. IT Governance, Risk and Compliance Policy

Environment, higher business complexity and increased focus on accountability have led us to pursue a broad range of IT governance, risk and compliance initiatives across the organization. We define IT Governance, Risk and Compliance Policy as a system of people, processes, and technology that enables an organization to:

- Understand and prioritize stakeholder expectations.
- Set business objectives that are congruent with values and risks.
- Achieve objectives while optimizing risk profile and protecting value.
- Operate within legal, contractual, internal, social, and ethical boundaries.
- Provide relevant, reliable, and timely information to appropriate stakeholders
- Enable the measurement of the performance and effectiveness of the system.

In our IT Governance, Risk and Compliance Policy is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity.

In our IT Governance, Risk and Compliance Policy represents the capabilities that integrate the IT governance, management and assurance of performance, risk and compliance activities Policy Statement.

In our IT Governance, Risk and Compliance Policy is viewed as an integrated collection of all capabilities necessary to support Principled Performance and does not burden the business, it supports and improves it.

9. Respond to business risks related to Information Technology in real-time

Our IT Governance, Risk, and Compliance helps transform inefficient processes across extended enterprise into an integrated risk program. Through continuous monitoring and automation we deliver a real-time view of compliance and risk, improves decision making, and increases performance across organization and with vendors. Organization connect the business, security, and IT with an integrated risk framework that transforms manual, siloed, and inefficient processes into a unified program built on a single platform.

10. Framework for Effective IT Governance, Risk and Compliance Policy

11. Responsibilities

The IT Governance, Risk and Compliance Policy Board is responsible for:

- Setting objectives for organization
- Delegating authority, setting limits of acceptable behavior through the Code of Conduct and defining risk appetite and tolerance by approving our Policies
- Establishing and monitoring effective IT governance, risk and compliance management.

12. Executive Management (individually and as a team) is responsible for

- Achieving objectives set by the Board and managing uncertainty in relation to these objectives
- Promoting a performance culture embedding risk management in decision making and business processes
- Creating awareness of and ensuring compliance with legal, regulatory and other obligations
- Keeping the Board informed of risks and compliance issues and endorsing all information provided to the Board
- Establishing standards and procedures to underpin board approved our Policies
- Making available the necessary resources for effective IT governance, risk and compliance management

13. All employee/user (including third party vendor) are responsible for:

- Actively seeking to understand the objectives, risks, controls and obligations that relate to their activities and participate in governance, risk and compliance management
- Undertaking activities in compliance with legislation and our policies and procedures
- Identifying and reporting risk events and instances of non-compliance; and
- Reporting new risks, risks exceeding tolerance, breaches or weaknesses of controls to their supervisor and as required under our Policies

14. Governance, Risk and Compliance Team is responsible for

- Providing expert advice and support in relation to IT governance, risk and compliance management
- Establishing an Enterprise Risk Management and Compliance Framework that enables effective risk management and compliance activity to be carried out consistently across the organization
- Ensuring there is an appropriate level of understanding and engagement in risk and compliance management through effective education, reporting, escalation and discussion
- Establishing an IT Governance Management Framework which delegates authority, sets limits and describes risk tolerance (e.g. via policies, standards, procedures)
- Establishing a Business Continuity Framework to ensure risks that threaten the ongoing operation of the organization are effectively planned and managed
- The review and continuous improvement of this policy and governance, risk and compliance management across the organization
- Facilitating the process outlined within the Enterprise Risk Management and Compliance Framework and ensuring the ongoing reporting of the outcomes of those processes.

15. Contact Information

Any Issue regarding Governance, Risk and Compliance Policy, please contact systems@vakrangee.in

Vakrangee
सशक्त परिवर्तन

CORPORATE OFFICE:
Vakrangee Corporate House,
Plot No. 93, Road No. 16, M.I.D.C.,
Marol, Andheri (East),
Mumbai – 400093, Maharashtra