TeamLease® RegTech
Helping India Comply

The Compliance Blind Spot in Indian Enterprises

How Indian Enterprises Are Non-Compliant by Accident and What Boards Must Do Before Regulators Do

Rishi Agrawal
Co-founder and CEO, TeamLease RegTech

Over the years, I have seen one pattern repeat itself across organisations of every size. Compliance risks are often taken lightly, not because companies do not care but because the scale is enormous. Thousands of obligations, multiple laws, endless filings, licences, registers, inspections and deadlines make it easy to assume that everything is under control. But hope is not a strategy and ignorance is not a solution. The real problem is that non-compliance is often invisible. It hides in day-to-day operations through a missed renewal, a wrong register format, excess gas cylinder storage, poor contractor records or unsafe workplace practices. These may seem like small gaps and are easy to ignore until they become expensive. One inspection, one notice or one incident can suddenly lead to financial loss, operational disruption, reputational damage and sometimes even personal liability for management. Today, boards and leadership teams cannot afford to look away. They are expected to know what is happening on the ground not just what appears in reports. At the same time, compliance obligations keep changing. Regulations evolve constantly, enforcement is becoming digital and data-driven and expectations from businesses are rising. Compliance today is no longer just a checklist activity. It has become a core business risk. The good news, however, is that most compliance failures are preventable. The right digital guardrails, trained people, strong management oversight and regular compliance audits can significantly reduce risk. More importantly, audits help uncover hidden gaps, test ground reality and fix issues before regulators find them.

At TeamLease RegTech, this is exactly where we support organisations. We help businesses identify what is being missed, address it in time and stay prepared in a constantly changing regulatory environment.

Because in compliance, what you cannot see is often what hurts the most

Table of Contents

Compliance Audit ≠ Other Audits

Existing audits do not equal compliance assurance

A common response from boards and independent directors, when asked about the last compliance health check, is to point to the multiple audits already being conducted, statutory audits, internal audits, ISO or operational audits, often led by large and reputed firms. However, this reflects a fundamental misunderstanding. These audits, while critical, do not substitute for a compliance audit. Statutory audits are primarily concerned with financial reporting, taxation, and the accuracy of books of accounts. Internal audits focus on process gaps, adherence to standard operating procedures and potential operational or reputational risks. ISO and similar audits assess the quality of products, services, and operational standards. None of these, however, are designed to comprehensively evaluate an organisation's adherence to the full spectrum of applicable laws. A compliance audit is distinct in both scope and intent, it examines the law of the land, covering all applicable regulations across central, state and local levels, spanning multiple categories of laws and diverse compliance requirements relevant to the entity's operations. For organisations operating in India's complex regulatory environment, this distinction is critical, as the absence of a dedicated compliance audit leaves a significant layer of legal and regulatory risk unaddressed.

How Non-Compliance Actually Happens on the Ground in Companies?

Compliance within enterprises is often understood as a collection of filings, licences and periodic checks. In reality, compliance risk does not arise uniformly. It is structurally skewed, driven by how different types of obligations behave in practice.

1. Four Types of Compliance

Enterprise compliance obligations fall into four broad categories:

- Time Based

Periodic and recurring obligations such as filings, returns, registers, and disclosures

- Event-Based

Triggered by specific events such as registrations, changes in structure, incidents, or regulatory actions. These are of two types- secretarial and non-secretarial

- On going

Continuous obligations that must be maintained during day-to-day operations. Examples include workplace lighting, temperature and ventilation standards, maintenance of statutory registers, safety equipment, welfare facilities and other operational requirements. While individual instances may appear low risk, their large volume and physical nature can create significant exposure during inspections.

- License based

These are based on the ones under which licenses are to be obtained or renewed for a specific business purpose

2. The 70-30 Risk Reality

Non-compliance risk is not evenly distributed across these categories.

Based on observations from compliance audits and assessments, event-based, licence-related and operational compliances account for a significant majority of compliance risks, often estimated at around 70%, while periodic filing-related risks account for the balance.

As a result, enterprises that maintain strong filing discipline may still face significant compliance exposure if operational conditions, licence requirements and event-based obligations are not actively monitored.

3. Compliance Risk Often Begins with Incorrect Applicability Assessment

Before any compliance obligation can be fulfilled, an organisation must first determine whether it applies. Many compliance failures arise not from poor execution but from an incorrect assessment of statutory triggers, thresholds, or applicability conditions. A common misconception across enterprises is that compliance applicability can be influenced through physical structuring or operational arrangements. Whereas applicability is determined by statutory thresholds, technical specifications, quantities, capacities and other conditions prescribed under law, not by how assets are arranged or distributed.

Understanding these triggers is critical because an incorrect applicability assessment can create compliance gaps long before a filing is due or an inspection takes place. The following examples illustrate how compliance obligations are determined by statutory criteria rather than organisational assumptions.

Boilers:

Under the Boilers Act, 1923, applicability is determined based on:

- Pressure
- Capacity
- Steam generation characteristics

Physical separation alone does not determine applicability. Each boiler is assessed against statutory definitions and technical specifications prescribed under the law.

It may create multiple independent compliance obligations.

Gas Cylinders:

Compliance depends on:

- Quantity stored
- Storage conditions
- Mode of usage

Licensing requirements depend on the quantity stored, storage arrangements and intended use. Thresholds prescribed under applicable regulations determine whether approvals or licences are required.

Configuration also matters. A connected system may be treated differently from stored units, depending on regulatory interpretation.

Ozone-Depleting Substances

The use of substances such as refrigerants is regulated based on environmental impact.

- Certain substances trigger compliance obligations due to their classification
- Alternative materials may reduce or eliminate regulatory exposure

The Physical & Infrastructure Blind Spot

The most critical compliance failures are not found in filings or documentation. They exist in physical conditions and operational reality.
These failures are typically identified only during on-ground inspection.
What Compliance Audits Detect During Physical Inspection

Registers and Records

- Non-maintenance of statutory registers in prescribed formats
- Use of loose sheets instead of bound registers
- Incomplete or backdated entries

Displays and Disclosures

- Absence of mandatory statutory notices
- Outdated or incorrect disclosures

Licence Conditions vs Actual Operations

- Licences obtained but conditions not implemented
- Operational limits exceeded beyond approved thresholds

Safety and Hazard Preparedness

- Absence of PPE kits in hazardous environments
- Missing eye wash stations
- Inadequate first-aid preparedness

Electrical and Emergency Preparedness

- Absence of emergency sand buckets or equivalent systems
- Inadequate emergency response infrastructure

Earthing and Electrical Compliance

- Tanks without double earthing
- Earthing pits not properly maintained or tested
- Mandatory annual testing not conducted

Fire Safety Systems

- Non-functional fire extinguishers
- Inadequate quantity or improper placement
- Lack of maintenance and inspection records

Structural Over-Compliance Creates Risk

A less visible but equally significant risk arises from how enterprises structure their compliance architecture.
In many cases, organisations increase the number of compliance units under the assumption that it improves control. In practice, it often has the opposite effect.

PF Code Fragmentation

Under the framework governed by the Employees' Provident Fund Organisation, organisations sometimes create multiple registrations across locations or units.
Observed Practice

- Separate registrations for different factories or offices
- Decentralised compliance ownership

Resulting Risk

- Increased number of filings
- Fragmented tracking
- Higher probability of missed or inconsistent compliance

Executive Summary

Compliance Audits are no Longer a Governance Hygiene Issue. They are an Enterprise Risk Issue

CORE INSIGHT

Non-compliance is not the exception in Indian enterprises; it is the default state. Most organisations discover this only at the point of regulatory action. At that point, remediation is no longer a choice but a settlement.

Section 134(5)(f) of Companies Act mandates directors of every company to make sure that proper systems have been implemented to ensure compliance

Indian enterprises operate under one of the densest and fastest-moving regulatory landscapes in the world, with more than 1,500 Acts and Rules, 69,000 compliance obligations, 6000 filings and approximately 13,000 regulatory changes occurring annually across nearly 3,750 government websites across central, state and local levels. The compliance governance model most enterprises deploy was designed for a regulatory environment that no longer exists.

The result is a systemic, invisible and compounding gap between compliance reporting and compliance reality. Compliance dashboards show green. Audit committees receive assurance and yet, when a regulator walks in, whether a factory inspector, a labour officer, an Extended Producer Responsibility auditor or the Enforcement Directorate, the gap becomes visible, expensive and personal.

Four findings leadership must confront

Finding 1 - Applicability Is Broken Before Execution Begins

Applicability mapping is the act of determining which laws apply to which entity, location and employee category. It is the single most important step in the compliance cycle and the most error-prone. In multi-state, multi-entity operations, applicability varies by plant, by contractor type and by local interpretation. The enterprise tracks what it believes is applicable. It does not track what the law actually requires.

Finding 2 - Periodic Audits Are Structurally Behind the Regulatory Curve

With around 13,000 regulatory changes per year, an annual audit is inspecting a calendar that is already obsolete. Quarterly audits are closer and still insufficient. Between audit cycles, applicability shifts, licences expire, notices arrive and new obligations crystallise. The enterprise has accumulated 90-270 days of undetected non-compliance by the time the next audit reports.

Finding 3 - The Anatomy of the Risk of Non-Compliance has to be identified

Compliance platforms play a critical role in structuring and tracking obligations, creating a system of record and improving visibility. They map applicability, assign ownership and capture evidence of compliance activities. However, they are not designed to independently verify compliance and therefore need to assess and map the risks accordingly.

Finding 4 - Non-Compliance Has Become Personal

Across key legislations of the country, more than 26,000 compliances carry imprisonment provisions for directors, Key Managerial Personnel and named officers. These liabilities do not sit on the balance sheet. They sit on individuals. Corporate indemnities do not travel to criminal dockets.

Business implications

- Director and officer exposure is a live, continuous liability across operating, labour, environmental and financial statutes.
- Non-compliance compounds. A single labour violation triggers a factory notice, which triggers an environmental inspection, which triggers a tax or FEMA enquiry. Enterprises underestimate the cascade.
- ESG, investor due diligence, IPO readiness, private credit covenants and merger and acquisition processes now demand independently validated compliance positions. Self-certification is no longer accepted.
- The cost of non-compliance is increasingly operational, not financial. Licence suspensions, plant shutdowns, consent withdrawals and export blocks disrupt revenue at a scale that dwarfs the underlying penalty.

What leadership must do, now!

- Commission an independent, enterprise-wide compliance audit covering applicability, evidence and on-ground reality across every entity, location and contractor relationship. Do not accept self-certification from the teams whose performance the audit assesses.
- Institutionalise continuous compliance assurance. Separate monitoring (what tools do) from validation (what audits do). Both are necessary, neither substitutes for the other.
- Elevate compliance from a functional activity to a board-owned risk. Define ownership, escalation and exception protocols. Report to the audit committee quarterly with evidence and not assertions.

THE BOARD QUESTION

*"**Across all our entities, plants, and contractor relationships, are we inspection-ready today and how do we know?"***

Audit readiness requires more than reported compliance, it requires evidence that has been independently validated and, where relevant, physically verified.

01

Compliance Is Integral to Business Operations in India

Scale, fragmentation and the continuous nature of statutory obligations

WHAT IS HAPPENING?

India operates one of the most complex regulatory environments in the world: 3 levels of the government, 7 Categories of the Law, 21 Regulatory Instruments, 42 Types of Compliance, 1,500+ Acts and Rules, 69,000+ Compliance Obligations and 6,618 Filings

WHY IT MATTERS?

Scale alone is not the issue. Fragmentation is. The same enterprise is simultaneously Union-regulated, State-regulated and Locally-regulated, each with independent enforcement, independent penalties, and independent timelines

RISK IF IGNORED

An enterprise that manages its regulatory landscape at a national level but not at a state and plant level is not compliant. It is merely aggregating it non-compliance. Regulators inspect locally, not nationally

1,530+
Acts & Rules in force

69,000+
Compliance obligations

13,000+
Regulatory changes per year

3,750+
Government websites issuing rules

26,000+
Clauses with imprisonment provisions

40+
Compliance types - from licences to registers

1.1 India's Wide Regulatory Landscape

Compliance obligations in India move across Union, State and Local tiers — each generating its own independent stream of instruments. Seven broad categories of law govern enterprise operations: Finance and Taxation, Secretarial, Commercial, Industry-Specific, Environment, Health and Safety, Labour, and General. These obligations arrive through 21 distinct instruments — Acts, Rules, Circulars, Notifications, Office Memorandums, Government Orders, Guidelines, Press Releases and more.

Each instrument carries different legal weight, different compliance timelines, and different evidentiary standards. State-level interpretation varies meaningfully: what is compliant in Maharashtra does not transfer to Tamil Nadu without a fresh applicability assessment.

Enterprises that monitor only primary Acts routinely miss subordinate instruments- municipal notifications, pollution board circulars, fire authority mandates through which most operational disruptions are actually enforced.

1.2 Keeping Up with Continuous Regulatory Change

India generates thousands of regulatory changes every year. Last year, there were 13,000 regulatory changes across 3,756 government websites- 584 Union, 2,083 State, and 1,091 Local. These changes include penalty revisions, frequency adjustments, form changes, rate revisions and entirely new legislation.

A quarterly review cycle absorbs 3,250 changes between reviews. An annual cycle absorbs all 13,000.

The gap between how fast the regulator moves and how fast the enterprise's review cycle moves is the definition of the exposure window. That window is where enforcement lives.

The gap between how fast the regulator moves and how fast the enterprise's review cycle moves is the definition of the exposure window. That window is where enforcement lives.

1.3 Compliance Failures Can Lead to Criminal Liability

Unlike many jurisdictions where non-compliance resolves through corporate fines, Indian law operationalises compliance through personal liability. More than 26,000 statutory clauses carry imprisonment provisions, with directors, KMPs, Occupiers under the Factories Act, Principal Officers under labour law, Compliance Officers under SEBI regulations and Data Protection Officers under the DPDP Act personally named as responsible parties. The enterprise does not go to jail. Its officers do.

Enforcement has moved from exceptional to routine. Factory inspectors, pollution control boards, GST officers, ESIC inspectors, labour commissioners, the Registrar of Companies, and sector regulators now operate at a frequency, scrutiny depth and willingness to prosecute that was not present even five years ago.

1.4 Compliance Obligations Have Different Timelines

Compliance is not one homogeneous activity. It includes licences and registrations, filings and returns, statutory payments, physical and infrastructure standards, statutory appointments, and responses to notices and orders.

Each carries different ownership, different legal weights, and different evidentiary standards. The evidence standard that applies to a tax payment is not the standard that applies to machine guarding on a factory floor. Audit approaches that apply a single methodology (e.g., document upload) to all 41 compliance types structurally fail to validate at least half of them.

1.5 How Compliance Varies Across Operational Units

Even in structured corporate environments, compliance levels range between 61% and 79%, with warehouses showing the weakest adherence. This indicates that non-compliance is not incidental but systemic across unit types. Refer to the table ahead.

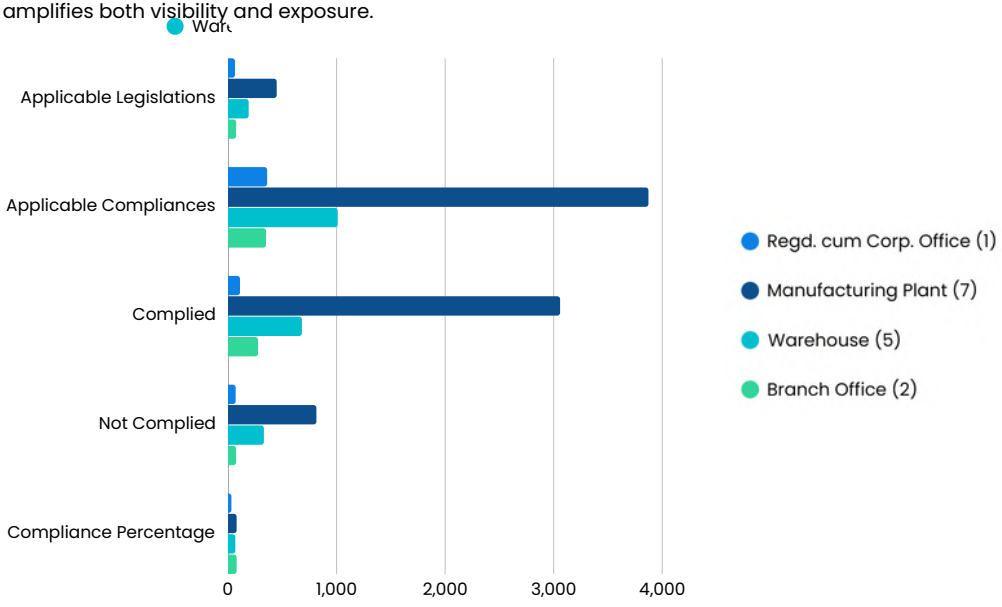
Unit Type*	Applicable Legislations	Applicable Compliances	Complied	Not Complied	%
Registered Office	62	323	244	79	75%
Manufacturing Plant	63	433	343	90	79%
Warehouse	36	198	121	76	61%
Branch Office	37	180	124	57	70%

Source: TeamLease RegTech Database; analysis based on compliance audits conducted for select enterprises
Assumption: The analysis is based on a representative enterprise footprint comprising 22 shops and establishments and 47 plants across geographies

To illustrate how compliance gaps manifest across enterprise structures, two case studies, a large auto-component manufacturer and a small-sized pharma company, were analysed across unit types by our research and implementation teams. The findings reinforce that non-compliance is not uniform rather it varies significantly by scale, operational

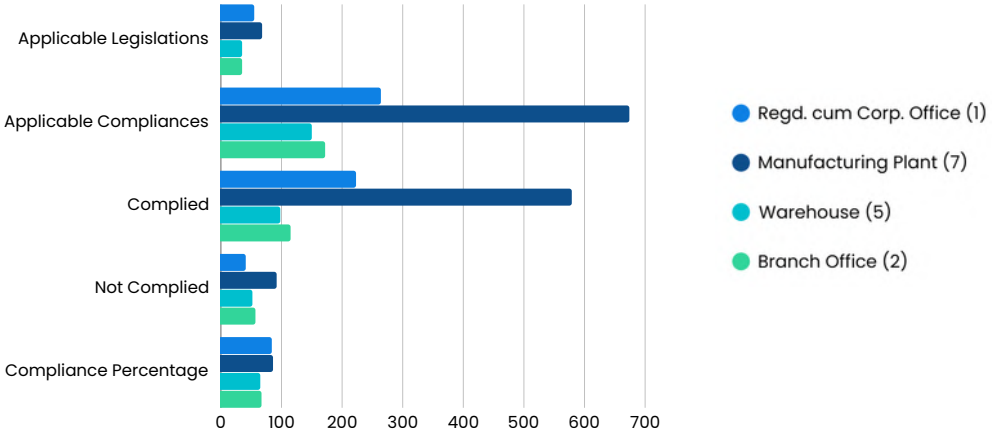
Case Study 1: Large Auto Component Enterprise

In the large enterprise context, manufacturing units show relatively higher compliance (79%), but this masks significant gaps in warehouses (67%) and even registered offices (31%), where applicability complexity is highest. The scale of operations (7 plants, 5 warehouses) leads to over 3,800 compliance obligations, with more than 800 instances of non-compliance demonstrating how scale amplifies both visibility and exposure.



Case Study 2: Small Size Pharma

In contrast, a small-sized pharma enterprise shows higher overall compliance levels (84-86% in core units), but with notable gaps in warehouses (65%) and branch offices (67%). Despite a smaller compliance universe, the persistence of gaps across unit types indicates that lower scale does not eliminate compliance risk, it merely reduces its visibility and volume.



The case studies show that non-compliance is rarely caused by a single lapse. It typically emerges from a combination of structural and operational gaps that vary by unit type, size and location. In larger establishments, the complexity is driven by a wider contractor ecosystem, multiple sites, higher physical infrastructure exposure and greater variation in state-level requirements. In smaller establishments, the challenge is often different but equally material, with issues arising from applicability misinterpretation, missed filings, incomplete documentation and diffused ownership of compliance responsibilities.

A critical underlying factor across both is the dynamic and fragmented regulatory environment. Frequent regulatory updates issued across thousands of websites at the union, state and local levels continuously alter compliance requirements, including changes in forms, formats, statutory calculations, due dates and filing frequencies. In the absence of a centralised tracking mechanism, these changes are often missed, leading to unintentional non-compliance. This is further compounded by the inability to systematically monitor licence and approval lifecycles, resulting in expiries or lapses that remain invisible until inspections or enforcement actions.

Across organisations, compliance is still largely treated as a documentation or event-based exercise rather than a continuously validated obligation. As a result, licences, consents, registrations, contractor obligations, regulatory notices and on-ground conditions are not tracked in an integrated manner. The gap is not just in execution but in visibility, where what is assumed to be compliant diverges from what is legally enforceable.

Importantly, the risk is not merely procedural. A significant proportion of these obligations carry provisions for imprisonment, elevating the consequences from financial exposure to personal liability for management. As highlighted in the monograph Jailed for Doing Business by Rishi Agrawal and Gautam Chikermane, India's regulatory framework historically embeds criminal liability even for procedural and technical lapses, exposing directors and key managerial personnel to prosecution risk. For boards, this reframes compliance from an operational checklist to a governance priority with direct implications for fiduciary responsibility and oversight.

The tables therefore reflect more than missed compliances; it highlights a systemic gap between perceived compliance and actual legal adherence in an increasingly complex and real-time regulatory environment.

02

The Most Overlooked Areas of Compliance

Contractors, applicability, state variation, licences, notices and orders

WHAT IS HAPPENING?

Enterprises over-monitor high-visibility obligations returns, filings, listed-company disclosures and systematically under-monitor the obligations that regulators actually enforce on-site

WHY IT MATTERS?

Visibility is correlated with internal reputational stakes, not with external enforcement risk. The most under-audited compliance categories are also the ones most likely to trigger inspection, licence suspension, or criminal prosecution

RISK IF IGNORED

A compliance programme that is strong on the things the CFO can see, and weak on the things the Factory Inspector can see, is a compliance programme that optimises for internal assurance at the cost of external survival

2.1 Contractor Compliance Remains a Major Risk Area

Under Indian law, the principal employer carries direct statutory liability for contractor non-compliance across Provident Fund (PF), Employees' State Insurance (ESIC), and the payment of wages. This liability is not merely a contractual risk but a statutory mandate; the commercial arrangement does not transfer this burden, as liability follows the law rather than the contract. In practice, many enterprises treat contractor compliance as a contractual matter managed through indemnities and purchase orders rather than as a statutory obligation requiring active oversight. However, corporate indemnities do not extend to criminal dockets or statutory penalties.

The scale of this exposure is significant, as the full contractor ecosystem including security, housekeeping, logistics, manpower, maintenance, and project contractors, often accounts for 40% to 70% of the total workforce on-site. Despite representing a disproportionately higher share of compliance exposure, this segment is rarely integrated into the enterprise's core compliance monitoring platform. A robust audit must therefore encompass the end-to-end contractor universe, covering the following critical areas:

- Statutory Contributions (PF and ESIC): Organisations often assume contributions are deposited based on contractor invoices, but independent verification at the UAN level and contribution matching are rarely performed.
- Wage Compliance: Any shortfall, delay, or non-payment of minimum wages, overtime, or bonuses creates direct liability for the principal employer, regardless of the contractor's internal processes.
- Contract Labour Compliance (CLRA and Allied Laws): While licensing and registration are often documented at contract execution, the ongoing maintenance of statutory registers and compliance with engagement conditions are frequently unmonitored during the contract lifecycle.

The result is a high-volume, low-visibility risk layer where compliance is frequently assumed rather than independently verified. Because these high-risk obligations often sit outside the software's line of sight, they represent one of the largest hidden liabilities in Indian enterprises today.

2.2 Gaps in Licences, Consents and Filings Create Compliance Risks

Enterprises often treat licences, consents, registrations, and filings as the same. They are not. Each has a separate lifecycle, documentation requirement, and enforcement trigger. Treating them as one category creates compliance gaps.

A renewed licence does not fix a lapsed consent. A filed return does not replace a missing registration. Most systems still track compliance as events, renewals and filings. Regulators check continuous validity and conditions. This mismatch leads to errors. Teams submit the wrong documents or assume compliance is complete once recorded.

The gap becomes visible during expansion or operational changes. Enterprises track primary licences but miss secondary and conditional approvals. These approvals are independently enforceable and usually surface during inspections.

Commonly missed or lapsed approvals:

- Groundwater NOCs
- BOCW registrations
- Fire NOCs
- ISMW registrations
- Waste management authorisations (hazardous, biomedical, plastic, e-waste)
- EPR obligations
- DG or solar approvals
- Lift and escalator approvals
- Vehicle fitness certifications

Enterprises also assume compliance depends on activity. This is incorrect. Several obligations apply even when there is no activity. POSH and Maternity nil returns and International Workers filings under PF are commonly missed, as the absence of activity is incorrectly treated as exemption rather than a reporting requirement.

Commonly missed formal appointments:

- Electrical Safety Officers
- Grievance Officers (labour and IT frameworks)
- POSH Internal/Complaints Committees

These gaps exist because systems track documents, not obligations. They do not clearly separate licences, consents, and registrations. They do not link approvals to operational changes. Ownership is split across teams. Nil obligations are not included in compliance calendars.

2.3 Regulatory Notices and Orders Are Often Poorly Tracked

Regulatory action rarely starts with a penalty. It starts with communication- show-cause notices, summons, deficiency letters, inspection reports, and demand orders. These arrive through multiple channels: physical post, email, regulatory portals, or during inspections.

Most enterprises do not maintain a central record of these communications. Notices reach plants or units and stay there. Local teams respond, but the information does not move upward. Head office remains unaware of what is happening on the ground. The issue is lack of consolidation. Enterprises do not log notices across locations in one system. As a result, they cannot standardise responses or track repeat queries from the same authority.

This leads to a fragmented view of enforcement.

- Inspection findings treated as one-off events
- No linkage between repeated notices from the same regulator
- No visibility on escalation from advisory to enforcement

Regulatory action follows a clear sequence. Demand orders usually come after repeated deficiencies and inspection findings. When these are not tracked together, enterprises lose the opportunity to act early. In many cases, leadership becomes aware only at the final stage—when a penalty, demand order, or prosecution is issued. This creates a reactive model. Responses vary across locations, visibility comes too late, and costs increase. By the time action is taken, penalties have compounded and operations may already be disrupted.

2.4 State-Specific Compliance Requirements Are Frequently Overlooked

Enterprises often assume central laws apply uniformly across locations. They do not. Most laws operate through state-specific rules, notifications, and practices. Requirements vary by state- forms, registers, renewal timelines, and supporting documents differ. What works in Maharashtra may not work in Gujarat, Tamil Nadu, or Karnataka.

Most organisations still use a single national template. This creates consistency, but not accuracy. A process that is compliant in one state can fail in another due to differences in format, frequency, or documentation. Local authorities may also apply their own interpretations, which adds another layer of variation.

State-level regulation also changes frequently. Amendments, new forms, and local circulars are issued regularly. Enforcement focus differs across states. A one-time assessment becomes outdated quickly if it is not actively tracked.

Where this breaks down:

- State-specific requirements are not built into compliance systems
- Central teams push uniform processes without local validation
- Updates at the state level are not tracked in real time

The impact is structural. Applicability is assessed incorrectly. Required obligations are missed. Registers do not match local formats. Documents submitted during inspections get rejected. Internally, everything appears compliant. At the local level, it is not.

2.5 Incorrect Applicability Assessment Drives Compliance Failures

Every compliance framework starts with one question: what applies. This depends on the entity, location, workforce, processes, and scale. It defines the entire compliance scope. If an obligation is marked as not applicable, it is never tracked or executed. Most organisations treat applicability as a one-time exercise during setup. They reduce complex conditions to static checklists. These assumptions are rarely reviewed.

As operations change through expansion, workforce shifts, new processes, or regulatory updates applicability is not reassessed with the same rigour. The framework continues to run on outdated assumptions. The same teams define applicability and execute compliance. There is no independent validation. Incorrect exclusions continue, and new triggers are missed.

Where applicability errors commonly occur:

- Threshold-based laws (employee count, turnover, capacity)
- Contractor and third-party workforce deployment
- Hazardous or regulated processes
- Environmental impact and waste categories
- Workforce composition (gender, international workers)
- Sector-specific or activity-based regulations

2.6 Physical Infrastructure Compliance Is Often Overlooked

The most significant compliance risks are often not found in filings or documentation. They exist on the ground within physical conditions, infrastructure, equipment, and day-to-day operations and can only be identified through physical inspection and operational verification.
Most organisations treat compliance as complete once a task is marked, a return is filed, or a document is uploaded. Regulators do not. Regulatory inspections focus on whether statutory conditions actually exist, are operational, and are being continuously maintained.

An expired fire extinguisher, a blocked emergency exit, an unguarded machine, or the absence of mandatory safety infrastructure constitutes immediate non-compliance, irrespective of whether corresponding records or approvals exist on paper. Such failures can lead not only to penalties but also operational stoppages, suspension of licences, or regulatory escalation.

This gap is most visible in areas relating to health, safety, environmental management, and infrastructure readiness. Medical examinations may be irregular or inadequately documented. First aid preparedness is often inconsistent. Fire safety systems may exist but remain poorly maintained, insufficient in number, or non-functional. Waste management practices show similar patterns, where segregation, storage, and disposal mechanisms are either incomplete or inconsistently implemented.

Infrastructure-linked non-compliance is equally common. Emergency exits may be obstructed or fail to meet statutory norms. Machinery may operate without adequate guarding. Electrical systems may lack proper earthing or periodic testing. Conditions attached to licences and approvals are frequently treated as one-time requirements rather than continuing obligations.

A compliance audit identifies these gaps not merely as operational deficiencies, but as statutory exposures that may remain invisible until a regulatory inspection occurs.

Common Observations During Physical Compliance Inspections:

Registers, Notices & Statutory Records

- Non-maintenance of statutory registers in prescribed formats
- Use of loose sheets instead of bound registers
- Incomplete, unsigned, or backdated entries
- Absence of mandatory statutory notices and disclosures
- Outdated or incorrect display requirements

Safety & Emergency Preparedness

- Expired or incomplete first aid kits
- No trained first aid personnel
- Missing PPE kits in hazardous establishments
- Absence of eye wash stations or emergency response arrangements
- Fire extinguishers, hydrants, and alarms in poor condition or inadequate quantity
- Non-compliant emergency exits and evacuation routes
- Absence of emergency sand buckets or electrical fire response systems

Electrical & Technical Infrastructure

- Tanks without mandatory double earthing
- Earthing pits not maintained or tested periodically
- Annual earthing testing not conducted
- Unsafe or exposed electrical systems
- Unguarded or unsafe machinery

Environmental & Operational Compliance

- Non-compliant waste storage and disposal systems
- Inadequate emission control systems or stack height deviations
- Improper operation or maintenance of ETP/STP systems
- Improper storage of petroleum, chemicals, or gas cylinders
- Boiler operations not aligned with statutory operating standards

Workplace Infrastructure & Welfare

- Inadequate disabled access provisions
- Absence of workforce welfare facilities, including female washrooms
- Non-compliant employee amenities and welfare infrastructure

2.7 Compliance Is Increasingly Real-Time and Event-Driven

Compliance no longer stays internal or surfaces only through periodic filings. Regulators now require real-time reporting, strict timelines, and public disclosure. The gap between an event and its consequence has reduced significantly.

SEBI Regulation 30 reflects this shift. It removes subjectivity and sets clear materiality thresholds. It mandates disclosure within 30 minutes to 24 hours. It also treats regulatory actions, penalties, and notices as inherently material. Even small penalties must be disclosed because they signal compliance discipline. This creates a direct link between operations and market perception. A delay in internal communication can lead to a disclosure failure. That delay itself becomes a separate non-compliance.

Other frameworks follow the same approach. Companies Act 2013 imposes daily penalties for delayed filings. It can escalate to director disqualification or company strike-off. Secretarial audits and auditor reporting requirements further reduce the ability to contain issues internally. Financial and cross-border compliance is also continuous. Under Foreign Exchange Management Act, 1999, export proceeds are tracked digitally. Delays are flagged through banking systems. Financial covenant breaches must be reported on time. There is little room for delayed detection.

Environmental compliance is now data-driven and disclosure-based such as Mandatory reporting through BRSR frameworks, Detailed environmental statements on resource use and emissions, Centralised reporting and verification under EPR frameworks. Workplace safety laws require immediate reporting of serious incidents. Delays are not permitted. In the digital space, Digital Personal Data Protection Act, 2023 mandates prompt breach notification followed by detailed reporting within strict timelines. Failure to report is treated as a separate violation.

Across frameworks, compliance has moved from periodic and document-driven to continuous and trigger-based. Events now flow directly from operations to regulators, and often to the market.

2.8 Many Compliance Obligations Fall Outside Formal Compliance Systems

Compliance in India does not sit under one framework. It spans multiple domains—labour, environment, safety, corporate, tax, sectoral, digital, and cross-border. Each operates independently, but failure in any one can trigger enforcement.

Workforce compliance itself is not limited to labour codes. It includes both new and legacy laws, along with social inclusion statutes that go beyond traditional HR requirements.

Key workforce and inclusion laws:

- Code on Wages, 2019, Code on Social Security, 2020, Occupational Safety, Health and Working Conditions Code, 2020, Industrial Relations Code, 2020
- Factories Act, 1948 and state Shops & Establishments laws
- Rights of Persons with Disabilities Act, 2016, HIV and AIDS (Prevention and Control) Act, 2017, Transgender Persons (Protection of Rights) Act, 2019

Environmental and safety compliance adds another layer. These laws require continuous monitoring, not one-time approvals.

Corporate and financial laws:

- Companies Act, 2013, Limited Liability Partnership Act, 2008, Insolvency and Bankruptcy Code, 2016

- Indian Contract Act, 1872, Competition Act, 2002
- Goods and Services Tax, Income Tax Act, 1961, Customs Act, 1962, Prevention of Money Laundering Act, 2002

Sector-specific laws add further complexity depending on the business.

Examples of sectoral laws:

- Legal Metrology Act, 2009
- Food Safety and Standards Act, 2006
- Drugs and Cosmetics Act, 1940

Digital and cross-border compliance continues to expand.

Key areas:

- Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023
- Foreign Exchange Management Act, 1999 and Foreign Trade (Development and Regulation) Act, 1992
- Prevention of Corruption Act, 1988 and Whistle Blowers Protection Act, 2014

2.9 Most Compliance Failures Originate from Operational Gaps

Most compliance gaps do not come from lack of legal knowledge. They come from poor execution. Policies exist, filings are done, and frameworks are documented. But implementation on the ground is inconsistent or not properly recorded.

Policies are a common example. Organisations maintain documents on safety, POSH, inclusion, and data privacy. But a policy alone is not compliance. Regulators check whether it is implemented and supported by evidence.

What regulators actually look for:

- Committees formally constituted
- Trainings conducted and recorded
- Roles and responsibilities clearly assigned
- Supporting records and documentation maintained

In many cases, the policy exists but the structure behind it does not. The same issue appears in disclosures. Laws require specific disclosures on websites, filings, and internal systems. These are often treated as one-time tasks. They are not updated or validated against current operations. As a result, disclosures exist but do not reflect reality.

In many cases, the policy exists but the structure behind it does not. The same issue appears in disclosures. Laws require specific disclosures on websites, filings, and internal systems. These are often treated as one-time tasks. They are not updated or validated against current operations. As a result, disclosures exist but do not reflect reality.

2.10 Understanding Event-Based and Condition-Based Compliance

Most enterprise compliance frameworks are built around event-based obligations- filings, renewals, payments, and disclosures because these are structured, trackable, and system-friendly. However, a smaller but critical segment of compliance is checklist- and condition-based, requiring physical verification, continuous maintenance, and on-ground validation.

This includes:

- Statutory registers maintained in prescribed formats
- Display requirements (abstracts, notices, licences)
- Health and safety conditions (machine guarding, emergency exits, first aid readiness)
- Environmental infrastructure (waste segregation, ETP/STP systems)
- Workplace facilities and amenities

While event-based compliances may constitute the majority of tracked obligations, checklist-based compliances often carry higher enforcement sensitivity because they are directly observable during inspections and an effective compliance audit is the only way to track it.

03

Understanding the Impact of Compliance Gaps

Financial, criminal, operational and reputational exposure

WHAT IS HAPPENING?

Penalties are one component of non-compliance cost. They are not the largest. Audit-compliance is cheap to produce but expensive to hold

WHY IT MATTERS?

The true cost is operational- licence suspension, consent withdrawal, plant shutdown, export embargo, listing consequences, investor exit, reputational spiral, and personal prosecution each of which is enforceable within days of a finding

RISK IF IGNORED

Leadership teams routinely benchmark exposure against historical fine ranges. That benchmark is obsolete. Enforcement now operates through operational disruption, not monetary penalty. The settlement is written in downtime

3.1 The Growing Financial Cost of Non-Compliance

Penalty regimes across GST, TDS, labour codes, and environmental legislation have been rationalised upward. This is compounded by a high compliance density; for instance, a typical MSME with over 150 employees faces 500 to 900 annual compliances, costing up to ₹18 lakh per year. Interest and daily-rate penalties convert small procedural lapses into material liabilities. In the finance and taxation category alone, 91% of imprisonment clauses now fall under GST rules, emphasizing the shift toward automatic, systemic enforcement.

3.2 Personal Liability for Directors and Key Personnel

According to the monograph, Jailed for Doing Business, authored by Rishi Agrawal and Gautam Chikermane, more than 26,134 statutory clauses carry imprisonment provisions, with 54.9% of all business laws containing at least one such clause. The responsibility is personal: Labour Law Intensity: Nearly 7 out of 10 imprisonment clauses (68.1%) are found in labour laws. Dissonance in Punishment: Under current laws, a business error of omission such as failing to whitewash a factory wall or maintain a spittoon can carry a punishment theoretically on par with serious crimes like sedition. State-Level Risk: 79.9% of these imprisonment clauses reside in state-level legislation, making local operations the highest risk point for personal prosecution.

3.3 The Business Impact of Compliance Failures

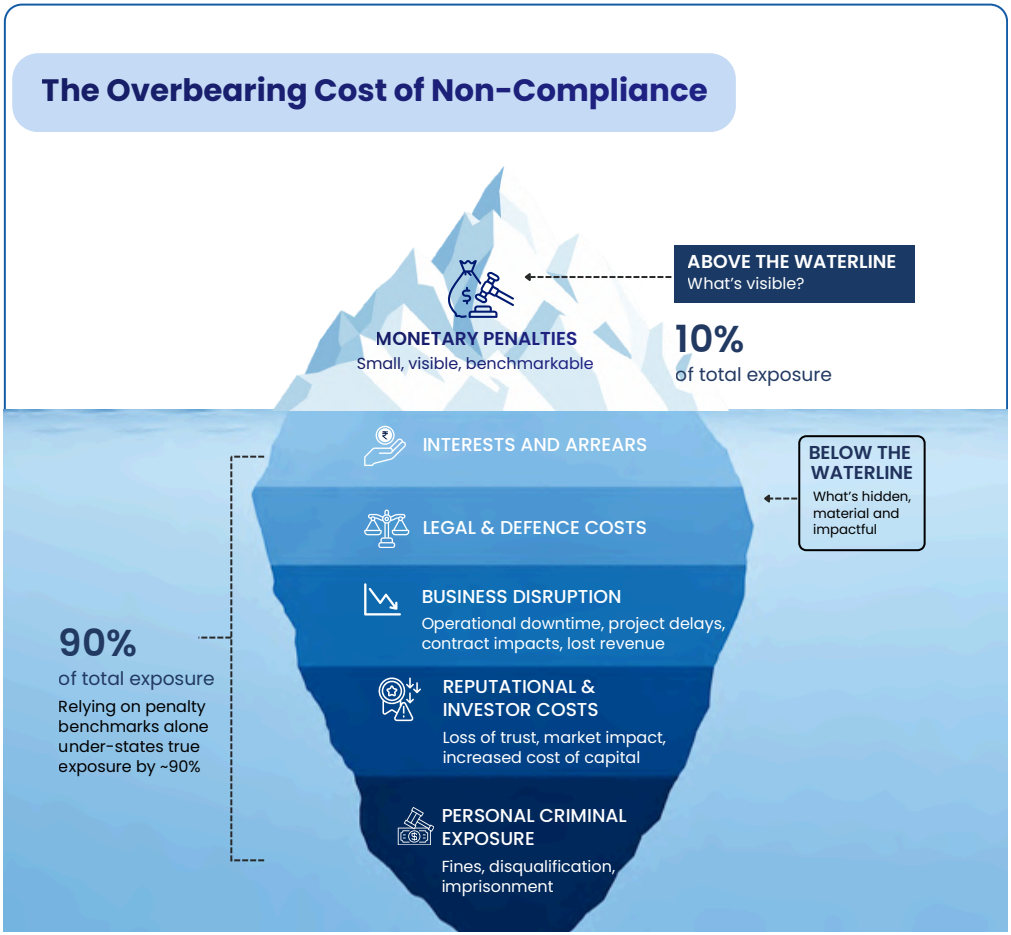
Regulators increasingly exercise operational powers. The "process is the punishment" when 37.8% of all business compliances carry potential jail terms. A technical breach in paperwork, such as failing to display an abstract of the Maternity Benefit Act carries the same coercive weight as a serious safety violation. These disruptions trigger immediate production losses and contractual defaults before any legal appeal can be heard.

3.4 Reputational and Investor Risks

Compliance events surface in investor due diligence and ESG ratings. As the monograph notes, this regulatory environment often forces entrepreneurs to stay small and remain under the radar to avoid the burden of over 400 new compliances that trigger immediately upon formalization or growth. For those who do scale, a single compliance failure becomes a capital event that discounts the entire enterprise valuation.

3.5 Compliance Risks Can Accumulate Across Multiple Laws

Non-compliance rarely stays contained. Modern enforcement follows a cross-regime pattern where a single inspection often cascades through several of the seven regulatory domains: Labour, Secretarial, Environment, Industry-specific, Finance, Commercial, and General. This regulatory cholesterol ensures that a wage register gap (Labour) can quickly escalate into a fit-and-proper question (Secretarial) or a tax mismatch.



04

Breaking Down the Risk of Non - Compliance

A risk heat map and compliance maturity ladder

4.1 High-risk compliance is difficult to fully digitise and verify

The obligations with the highest enforcement severity are often physical, site-specific and condition-based. Machine guarding, emergency exit readiness, first-aid preparedness, waste infrastructure and potable water quality require on-ground validation and cannot be reliably assured through document uploads alone. While digital tools can enhance visibility through geo-tagged evidence, sensors and audit trails, they largely depend on self-reported data. As a result, dashboards showing 100% compliance may reflect declared status rather than verified reality

Dimension	Compliance Platform	Independent Compliance Audit
Input	What the user enters	What the statute requires
Evidence	Sample documentation	Statutory registers, licences, filings, on-ground conditions
Applicability	As configured	Physically and independently validated per entity and location for as on date compliance status
Contractor ecosystem	Typically excluded	Fully scoped principal employer liability
Interpretation	Status tracking	Risk-ranked diagnostic
Value	Effective Compliance Management	Validated assurance

4.2 How do we at TeamLease RegTech like to look at non-compliance?

At TeamLease RegTech, we like to see several categories of compliance, occurrence and outcomes that get manifested.

The heatmap and maturity ladder below together provide a board-level lens to move from fragmented compliance visibility to a structured risk architecture. The heatmap disaggregates compliance into distinct exposure categories and evaluates each along three decision-critical dimensions: likelihood of occurrence, severity of consequence, and detectability. This framing helps separate noise from material risk. "Critical" exposures are not simply those with high regulatory importance, they are those where high probability intersects with high impact and low detectability, creating asymmetric downside. These are the areas where boards should expect proactive controls, independent validation, and frequent reporting. "Severe" and "Elevated" risks, while comparatively more detectable or less likely, still require systematic monitoring and clearly defined ownership, particularly where regulatory interpretation, contractor ecosystems, or state-level variability introduce structural complexity.

The following heatmap is a synthesis of commonly observed exposure patterns across mid-to-large Indian enterprises. It is indicative, not prescriptive an organisation-specific heatmap should be produced from its independent baseline audit. Bands: CRITICAL (active liability today), SEVERE (material and likely), ELEVATED (probable within 12 months), MODERATE (contextual), LOW (residual). (***An internal heatmap prepared by our team of 50 lawyers)***

Read: The exposures with the highest likelihood and highest severity almost always have the lowest detection in current audit models because they depend on applicability, on-ground verification, and contractor scope, all of which sit outside the compliance platform.

Risk Heat Map

Exposure Area	Likelihood	Severity	Detection	Exposure Band
Applicability misinterpretation	H	H	H	H
Contractor / principal employer liability	H	H	L	CRITICAL
Licence, consent, registration mismatch	H	H	M	CRITICAL
Physical infrastructure (guarding, exits, fire, first-aid)	H	H	L	CRITICAL
State-level variation in central laws	H	M	L	SEVERE
Statutory registers in prescribed format	H	M	M	SEVERE
Notices, orders, regulatory communication	M	H	L	SEVERE
Statutory appointments (Occupier, POSH, DPO etc.)	M	H	M	SEVERE
EPR / waste management (plastic, e-waste, battery)	H	H	L	SEVERE
Labour codes transition (wages, SS, OSH, IR)	H	M	M	ELEVATED
DPDP Act privacy policy, consent, grievance	H	M	M	ELEVATED
POSH Act committee composition and workflow	M	H	M	ELEVATED
GST reconciliation and ITC mismatch	M	M	M	ELEVATED
Secretarial filings and board procedure	L	M	H	MODERATE
SEBI disclosures (listed entities)	L	H	H	MODERATE

4.3 Compliance Maturity Ladder- to help you understand where you stand

A five-stage operating-model view of compliance maturity. Most large Indian enterprises operate at L2–L3 and self-assess at L3–L4. Independent baseline assessment typically relocates self-perception down by one to two stages. Movement up the ladder to L5 is governance-led, not technology-led.

From Reactive Chaos to Well-Governed Advantage

	What it looks like	Operating Reality	Risk Profile
LEVEL 1 AD HOC / PAPER-BASED (REACTIVE CHAOS)	• Paper-driven: drawers, files, scattered registers • "To whomsoever it may concern" titled compliance certificates • No systematic/assurance-based tracking of regulatory updates • No defined controls for vendor/contractor compliance • No training or awareness on compliance obligations • Filings done inconsistently, post-trigger • No senior management reviews on compliances	Compliance triggered by notices, inspections and crises	Maximum exposure: missed filings, penalties, prosecution risk
LEVEL 2 BASIC CONTROL / CALENDAR-DRIVEN (REACTIVE → PERIODIC)	• Static Compliance calendars (monthly/quarterly) • Some level of digitisation (Excel/tools) • Defined owners emerging • Basic documentation maintained • Limited regulatory update tracking	Scheduled compliance, not always complete/accurate	Moderate reduction; still vulnerable to regulatory changes
LEVEL 3 STRUCTURED / SYSTEMIC (CONTROL WITH GAPS)	• Policies, SOPs, ownership defined • Training programs implemented • Some digitisation (Excel/tools) • Compliance & risk registers maintained • Functional silos (HR, Legal, Ops) • Partial vendor compliance tracking • Limited regulatory update tracking • Periodic reviews (compliance audits)	Systems exist but in digital silos	Controlled but fragmented
LEVEL 4 INTEGRATED / CONTINUOUS (PROACTIVE CONTROL)	• Digital compliance management systems deployed • Real-time regulatory updates • Event-based triggers • Vendor compliance integrated • Periodic independent audits • Cross-functional alignment	Continuous monitoring replaces periodic checks	Significantly reduced; early issue detection
LEVEL 5 COMPLIANCE BY DESIGN (STRATEGIC & EMBEDDED GOVERNANCE	• Compliance embedded in business strategy • Compliance officer part of: • Product design • Market entry • New unit setup • Always audit-ready • Continuous audit & remediation • Vendor compliance lifecycle integration (documentation – is it reviewed or monitored on a regular basis or not?) • Board-level governance (is it aware as a quantitative posture of risk)	Compliance is part of the operating rhythm, embedded at stages of production and all consultations	Optimised risk, minimal surprises

	Leadership Visibility	Business Impact	Actionable Focus
LEVEL 1 AD HOC / PAPER-BASED (REACTIVE CHAOS)	False sense of compliance	High penalties, disruptions (such as management's bandwidth getting spent on firefighting with myriad problems), reputational damage	**Document & Organize** • Identify returns, registers, forms, formats, key obligations • Assign basic ownership
LEVEL 2 BASIC CONTROL / CALENDAR-DRIVEN (REACTIVE → PERIODIC)	Backward-looking reports	Operational inefficiencies, firefighting cost	**Plan & Track** • Build compliance calendar • Define owners • Start tracking updates
LEVEL 3 STRUCTURED / SYSTEMIC (CONTROL WITH GAPS)	Dashboard-driven; pockets of hidden risk	Better control, improved consistency	**Standardise & Strengthen** • SOPs, policies, training • Strengthen registers • Conduct periodic reviews
LEVEL 4 INTEGRATED / CONTINUOUS (PROACTIVE CONTROL)	Exception-based, evidence-backed	Lower compliance cost, faster decisions	**Integrate & Automate** • Centralised platform • Real-time monitoring • Event-based compliance
LEVEL 5 COMPLIANCE BY DESIGN (STRATEGIC & EMBEDDED GOVERNANCE	Real-time assurance; inspection readiness as KPI	Lower cost of capital Stronger regulator trust More management bandwidth	**Embed & Govern** • Integrate into strategy & lifecycle • Build governance frameworks • Ensure continuous readiness

05

What Does Effective Compliance Look Like?

A continuous, risk-based, accountable operating model

WHAT IS HAPPENING?

Current operating model: compliance is a residual output of distributed functional effort with audit as an annual check

WHY IT MATTERS?

Target operating model: compliance is an engineered, continuous capability with audit as a persistent, independent validation layer. The difference is organisational, not technological

RISK IF IGNORED

Enterprises that do not make the shift will continue to be non-compliant by design and will discover it only when a regulator, an investor, or an acquirer discovers it first

5.1 Building a Continuous Compliance Framework

Continuous compliance is not a quarterly audit run 12 times a year. It is a different operating model. It integrates regulatory intelligence, applicability assessment, obligation management, evidence capture, and independent validation into the daily operating rhythm of the enterprise not as a separate compliance function, but as a property of how work gets done.

In a continuous model, regulatory change is ingested in real time. Applicability is re-assessed whenever an operational event a new location, a new process, a new workforce category, a new vendor, a new product occurs. Obligations are triggered event-based, not calendar-based. Evidence is captured at the point of action, not reconstructed at the point of audit. And exceptions escalate automatically, not through manual reporting cycles.

5.2 Prioritising Risk-Based Compliance

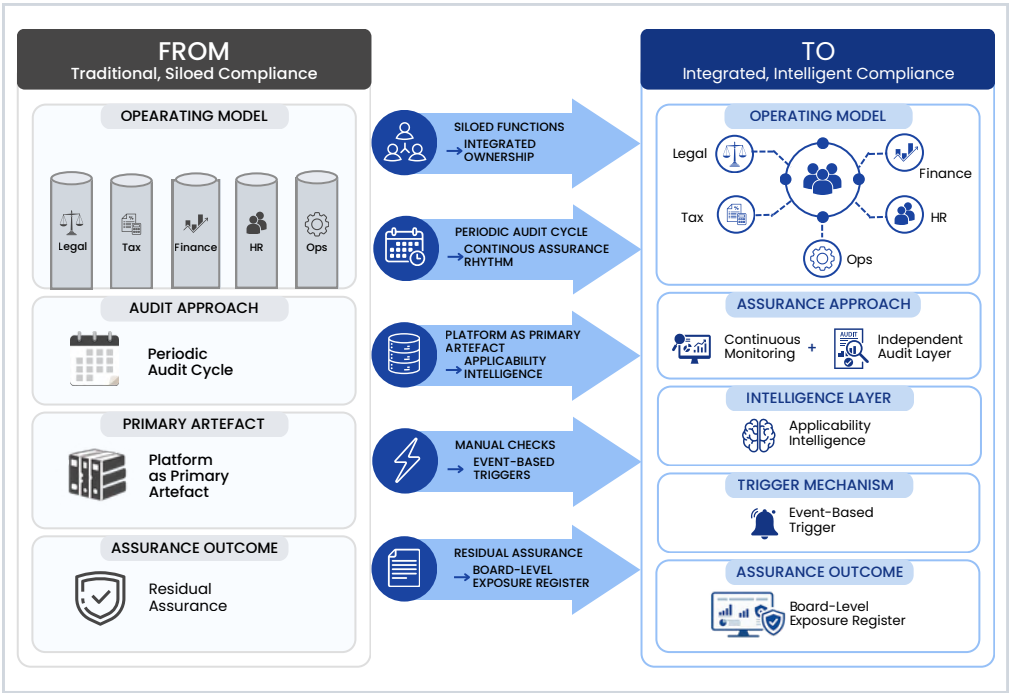
With 69,000+ obligations, no enterprise can treat compliance as an exercise in uniform coverage. Risk-based prioritisation focuses effort on the intersection of three conditions: likelihood of enforcement, severity of consequence, and weakness of existing control. The output is a ranked exposure list that leadership can act on not a comprehensive register that leadership cannot read.

5.3 Establishing Accountability and Oversight

Compliance by design makes ownership explicit at three levels: the operating owner (the person who executes), the accountable owner (the officer legally liable), and the governance owner (the board committee to which material exposure is reported). Escalation thresholds are pre-agreed: any Category A exposure (licence lapse, Occupier liability, consent withdrawal, criminal notice) goes to the Audit Committee within defined timelines, without discretion.

5.4 The Importance of Independent Compliance Validation

Continuous monitoring helps track compliance on an ongoing basis. Independent validation provides an objective review of that monitoring process, helping identify gaps, weaknesses, and areas that may have been overlooked. Both are essential and should operate together, not as substitutes for one another.



06

What a Robust Compliance Audit Must Cover?

Scope, depth, cadence and evidence standards

6.1 Comprehensive Compliance Coverage

A robust audit covers the full taxonomy of obligations. That taxonomy includes, at a minimum: licences and registrations (obtained, current, renewable); consents (to establish, to operate, withdrawal status); statutory filings (returns, reports, disclosures); statutory payments (taxes, duties, contributions, cess); registers and records (in prescribed formats, in the prescribed medium); statutory appointments (Occupier, Principal Officer, Safety Officer, Grievance Officer, POSH Committee, Data Protection Officer); displays and notices (on-site, prescribed); infrastructure standards (physical, measurable, inspectable); policy-level obligations (POSH, EHS, Equal Opportunity, HIV, Privacy, IT Act); notices and orders (received, responded, closed); and contractor and third-party obligations (end-to-end).

6.2 Entity-Level and Location-Level Compliance Mapping

Audit scope must cover every legal entity in the group and every operating location under each entity. Applicability must be assessed per legal entity and per operational location. An enterprise-level summary that applies a single national compliance template masks critical state-level variations and plant-level exposures. A robust audit decomposes to the unit of enforcement which is the local facility, not the corporate headquarters.

6.3 Including the Contractor Ecosystem in Compliance Assessments

Contractor compliance must be fully scoped as part of enterprise compliance due to principal employer liability. Audit coverage should extend to registrations, wage compliance, statutory contributions, and documentation across all contractors and locations.

6.4 Periodic Reassessment of Compliance Applicability

Applicability is not static. It shifts with workforce composition, process changes, geographic footprint, and regulatory updates. The audit must define the triggers under which applicability changes (e.g., crossing a headcount threshold or introducing a hazardous process) and document the logic used to arrive at the compliance map. An audit that does not test applicability hands the enterprise a map with an invisible expiry date.

6.5 Statutory Evidence and Documentation Standards

Evidence quality must be tested against what a regulator would accept including statutory registers in prescribed formats, original licences, complete audit trails, and on-site physical conditions. Accepting a photograph of a fire extinguisher or a sample PDF upload as proof of compliance is the starting point of an audit, not the end of it. Where the platform standard and the regulatory standard differ, the audit must report the gap.

6.6 Developing a Risk-Prioritised Remediation Roadmap

The output of an audit is not a list of findings. It is a ranked, time-bound, owned remediation plan with severity classification, root cause analysis, and closure validation. If the audit report ends at the list of findings, the audit has only documented the problem. It has not reduced it.

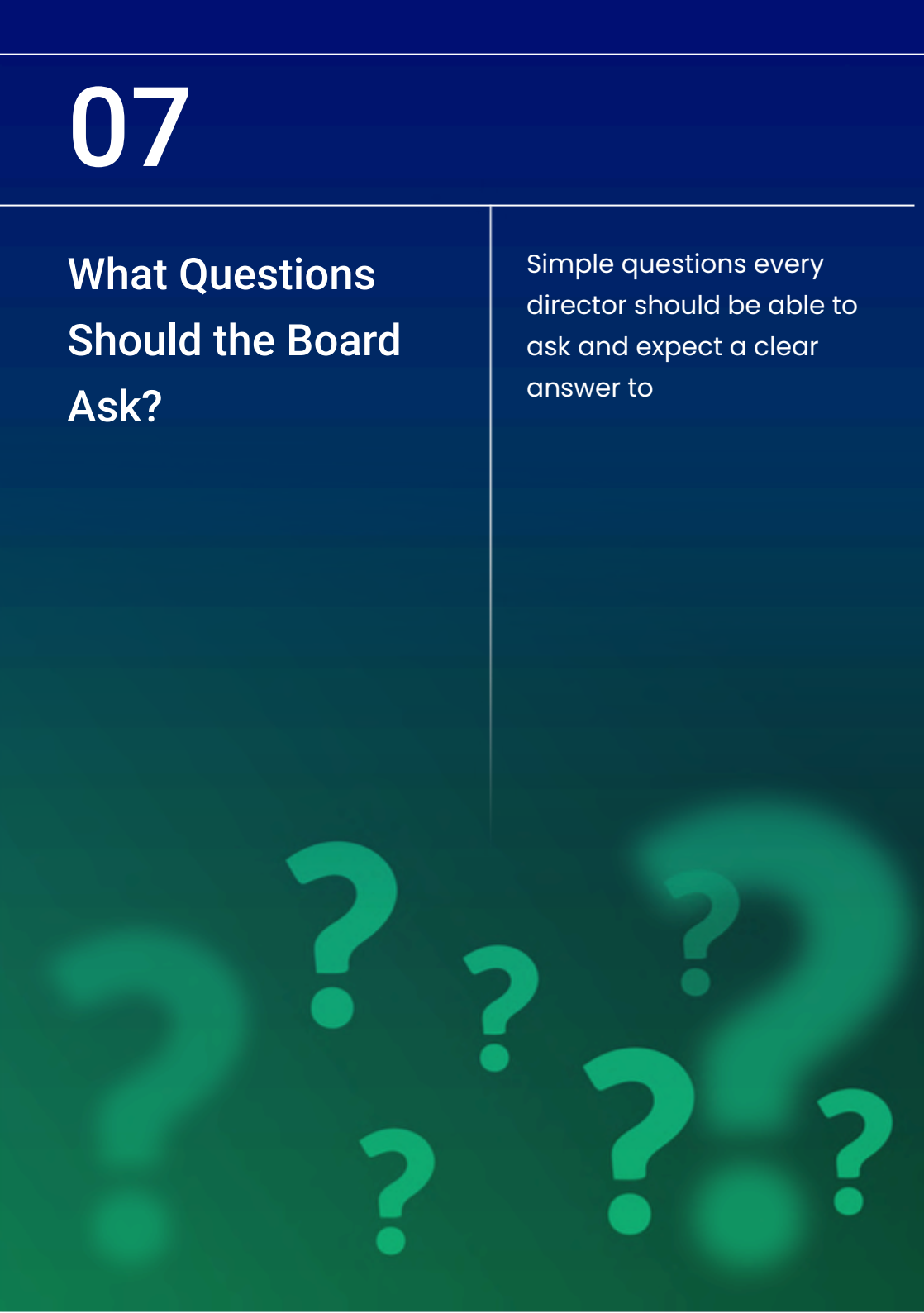
What should the audit cover?

Audit Dimension	Minimum Standard
Scope	All 41 compliance types, all entities, all locations, all contractors
Cadence	Continuous for high-risk categories, annual deep-dive for full universe
Depth	Applicability, evidence, on-ground, process, governance, root cause
Output	Risk-ranked roadmap with owners, timelines, and closure validation
Board linkage	Quarterly exposure view at Audit Committee. Material items direct to Board

07

What Questions Should the Board Ask?

Simple questions every director should be able to ask and expect a clear answer to



How to use this?

You do not need to be a compliance expert to use this list. Read these questions out in your next review. The aim is not to catch anyone out. It is to find out what is actually known, what is merely assumed, and what no one has checked. If the honest answer to a question is I assume so or the dashboard says so, that gap is exactly what this report is about

1. Do we actually know what applies to us?

- Do we have complete, current visibility into the laws applicable to each location, activity, and workforce category, including state-specific variations, and when was this last reviewed?
- How do we determine that a law is not applicable and is that decision independently validated and defensible in an audit, inspection, or due diligence?
- What triggers a reassessment- new geography, new activity, new process, or crossing a threshold like headcount or turnover and is this embedded into our change management?
- How do we continuously track and operationalise amendments, notifications and judicial interpretations as the regulatory landscape evolves?
- Do compliance, business teams, and leadership share a single source of truth for what applies, where and why?

2. Are we trusting reports that may not match reality?

- When reports show 100% compliance, does that reflect actual verification on the ground across factories, warehouses, and offices or just the completion of filings and tasks?
- How do we bridge the gap between compliance on paper and compliance in practice, and what independently validates that our controls are working?
- Between two audit cycles, what visibility does leadership have into emerging risks and has our compliance position ever been tested through third-party audits, forensic reviews, or mock inspections?
- Do our audits go beyond document verification to assess operational reality and do we have the right mix of expertise, technology, and advisory support to keep up with rising complexity?
- Can leadership get a single, evidence-backed view of compliance across locations and entities and are we investing enough in digitisation and continuous monitoring to make that possible?

3. Where Are the Compliance Blind Spots?

- How confident are we that we have visibility into our highest-risk compliance areas, especially the ones that rarely surface in board or management discussions?
- Are contractor, vendor, and third-party obligations- wages, social security, working conditions, statutory benefits- being actively monitored, given that non-compliance can trigger principal employer liability regardless of contract terms?
- Are all licences, registrations, permits, and conditional approvals being tracked through their full lifecycle, including location-specific permissions that are easy to overlook?
- Does our oversight extend beyond documentation to verify actual workplace conditions- safety, emergency preparedness, environmental controls, statutory records across remote sites, warehouses, plants, and third-party facilities?

- How effectively are notices, inspection findings, and operational compliance concerns escalated to leadership, tracked to resolution, and surfaced in dashboards alongside emerging risks, not just completed tasks?

4. What Does Non-Compliance Really Cost Us?

- If a regulator acted against us tomorrow, what would our true exposure be- operational, financial, reputational, and continuity, beyond monetary penalties?
- Are we assessing compliance risk based on statutory penalty amounts, or on how regulators are actually enforcing today?
- Which obligations expose directors, KMPs, occupiers, employers, or designated officers to personal prosecution or imprisonment and does our D&O cover that reality?
- Have we quantified the impact of non-compliance on investor confidence, fundraising, partnerships, customer trust and enterprise value?

5. Are We Built to Stay Compliant or Merely to Become Compliant?

- Is compliance embedded into day-to-day operations with continuous monitoring of obligations and emerging risks or do we engage with it mainly around audits, inspections, and reporting deadlines?
- For every significant obligation, is there clear ownership and accountability, and does a material gap automatically escalate to senior leadership and the board within a defined timeframe?
- Is our framework evolving at the pace of regulatory change, or are we still relying on compliance positions and interpretations established years ago?
- Do we have the right mix of people, process, technology, and governance to prevent issues proactively and to sustain compliance as the organisation grows?

6. Is Our Audit Program Testing What Truly Matters?

- Does our assurance framework specifically evaluate legal and regulatory compliance across all entities, locations, functions, and third-party operations or only a sample alongside financial and certification audits?
- Do audits verify legal applicability, evidence, and actual implementation on the ground, or stop at documentation review and self-certification by the teams executing compliance?
- Do audit outcomes result in clearly assigned corrective actions, timelines, and accountability with recurring gaps systematically tracked, analysed, and resolved?
- Does our framework assure future compliance resilience, or merely evaluate past performance?

7. Are We, as a Board and Leadership Team, Providing Effective Compliance Oversight?

- Have we obtained independent assurance on our compliance framework, and do the reports reaching leadership and the board offer verifiable evidence rather than status-based assurances?
- Is compliance a standing agenda item in governance and risk discussions, with sufficient visibility into our most significant risks and emerging exposures?
- Are concerns escalated proactively, or only after a notice, inspection, or enforcement action?
- If a regulator, investor, lender, or acquirer scrutinised us today, could we substantiate our compliance position with evidence and demonstrable controls and is compliance treated as a strategic governance priority, not just a regulatory obligation?

A Final Reflection

For each of these questions, the strongest answer is not simply yes. It is- Yes and here is the evidence. Any gap between assurance and evidence represents an area worthy of closer attention

08

Leadership Actions to Take Immediately

What Leadership Must Own

THE OPERATING PRESUMPTION

The question is not whether compliance gaps exist. In large, distributed Indian enterprises, they always do. The question is whether leadership knows what they are, has prioritised them, and is addressing them before a regulator, an investor, or an acquirer does

7.1 The three actions that define compliance governance maturity

Action 1 Commission an independent baseline audit this quarter
Scope: applicability, evidence, on-ground, contractor across every entity and every location. Independence: external of operating teams, external of the platform vendor. Output: a risk-ranked remediation roadmap reported to the Audit Committee within 90 days. Do not accept self-certification from the teams whose performance the audit assesses.

Action 2 Institutionalise continuous compliance assurance
Separate monitoring from assurance. Run them in parallel. Fund the assurance layer as a distinct governance capability not a line item in the compliance or legal budget. Hold the monitoring layer (platform, operations) and the assurance layer (audit) to different accountabilities and different reporting lines.

Action 3 Elevate compliance from a functional activity to a board-owned risk
Define ownership at three levels operating, accountable, governance. Pre-agree escalation thresholds. Report to the Audit Committee quarterly with evidence, not assertions. Make compliance a standing item in enterprise risk review. Make inspection-readiness an operating metric.

7.2 Role-specific decisions to make immediately

Role	Decision to take this quarter
Board / Audit Committee	Mandate an independent baseline compliance audit. Set the cadence of continuous compliance reporting. Approve escalation thresholds. Treat compliance exposure as a standing ERM item.
CEO	Name a single accountable owner for enterprise-wide compliance not for the platform, for the outcome. Make compliance an operating-committee standing item, not a quarterly summary.
CFO	Move compliance from a cost line to a risk line on the enterprise risk register. Quantify exposure financial, operational, personal with an independent view. Re-examine D&O and other insurance coverage against current criminal clause density.
General Counsel / CCO	Re-run applicability assessment across every entity and location. Scope contractor compliance in. Establish a single system of record for regulatory communication. Sequence remediation by regulatory consequence, not by internal convenience.
CHRO	Own labour, contract labour, PF/ESI, POSH, and workforce statutory appointments end-to-end including contractor ecosystem liability. Formalise the escalation path for plant-level incidents.
CIO / CDO	Ensure compliance platforms are fed by real-time regulatory intelligence, not manual update cycles. Close the integration gap between ERP, HRIS, EHS, and compliance systems. Separate 'status' from 'evidence.'
Plant Heads / Unit Heads	Treat every inspection real or simulated as an evidence test. Ensure statutory registers, physical infrastructure, and contractor records are inspection-ready on any given day, not only during audit windows.

Compliance is not complete until it has been tested

Audit is where compliance meets reality

CLOSING NOTE

This paper has not argued that digital compliance platforms are misguided they are, in fact, necessary. They streamline the flow of data and information, flag residual risks of non-compliance and identify delays that might otherwise go unnoticed. Yet necessary is not the same as sufficient. Compliance, at its core, remains a deeply human endeavour, one shaped by judgment, interpretation, ethical reasoning and the countless discretionary decisions that no system can fully automate or anticipate. Digital tools can surface the right information at the right time but it is people who must act on it, question it and ultimately own the outcomes. Continuous compliance assurance the combination of continuous monitoring, continuous regulatory intelligence and continuous independent audit must therefore be understood not as a technology project but as an organisational commitment, one in which platforms serve as enablers and people remain the final line of accountability

Strong compliance begins where independent audits ask difficult questions