

Risk • Pro

Building a trusted environment



RISKPRO MAGZINE 2026

CELEBRATING GROWTH AND PROGRESS IN 2025

TABLE OF CONTENTS:

Foreword & Leadership

1. Message from Leadership
2. Editor's Note

Data Privacy & Protection

1. DPDP Act in Practice: From Legal Text to Operational Reality
2. DPDP & Global Privacy Laws: Where India Aligns and Where It Differs
3. DPDP Compliance Readiness Checklist

Artificial Intelligence Governance

1. Artificial Intelligence – Regulatory Environment
2. AI Risks

Cybersecurity & Digital Risk

1. Cyber Risk in 2025: Why Prevention Alone Is No Longer Enough
2. Third-Party Risk: The Hidden Compliance Multiplier

Governance, Risk & Compliance (GRC)

1. Operational Resilience: Preparing for Disruption in an Interconnected World-Geo Political Risk
2. Key Regulatory & Risk Trends to Watch in 2026
3. Smart Resourcing for Risk & Cybersecurity Teams, presented by Riskpro India.

Labour Compliance & Workforce Governance

1. Labour Compliance as a Governance & ESG Issue
2. India's Labour Law Reforms: Are Organizations Truly Prepared?
3. Labour Law Compliance Audit – A Practical Guide

Riskpro Spotlight

1. What's New at Riskpro
2. Relixi
3. Partnership Program at Riskpro
4. Riskpro Academy
5. Building Expertise at Riskpro
6. Riskpro's 2025 Social Calendar: Building Connections, Sharing Knowledge, Celebrating Success

Looking Ahead

1. Riskpro's Vision for the Year Ahead

A WORD FROM THE CHAIR



WARM REGARDS,
MANOJ JAIN
CEO
RISKPRO RISK MANAGEMENT PVT. LTD.

MANOJ JAIN
CEO, RISKPRO INDIA

In today's rapidly evolving business environment, risk is no longer a peripheral concern it sits at the very core of strategy, resilience, and long-term value creation. As we release this year's edition of the Riskpro Magazine, I am proud to reflect on how far we have come and the direction in which we are headed.

The past year has been transformative. Regulatory developments such as the Digital Personal Data Protection Act, 2023 and continued global enforcement of the General Data Protection Regulation have reinforced the need for robust privacy governance. At the same time, the rapid adoption of artificial intelligence, expansion of digital ecosystems, and increasing third-party dependencies have redefined enterprise risk management.

Organizations are realizing that compliance alone is not enough. What is required is integration where information security, privacy, IT governance, labour law compliance, and operational controls work together within a unified risk framework.

At Riskpro, our mission remains clear: to help organizations build resilient systems, strengthen governance structures, and embed a culture of accountability. Over the past year, we have expanded our advisory capabilities, strengthened our audit practices, and deepened our partnerships to deliver practical, outcome-driven solutions.

This edition of our magazine captures the key themes shaping 2026 and beyond AI governance, data protection readiness, evolving compliance landscapes, cybersecurity resilience, and leadership perspectives from CISOs and compliance heads. I hope these insights serve not only as knowledge resources but as catalysts for meaningful action within your organizations.

I extend my gratitude to our clients, partners, contributors, and the dedicated Riskpro team. Your trust and collaboration continue to drive our growth and impact.

Together, we will continue to navigate uncertainty with clarity, discipline, and purpose.

EDITOR'S NOTE

As we present this year's edition of the Riskpro Magazine, I am reminded that the world of risk is no longer defined by isolated events it is shaped by constant change, interconnected systems, and emerging responsibilities.

Over the past year, we have witnessed significant regulatory evolution, particularly with the implementation of the Digital Personal Data Protection Act, 2023, increased global focus on privacy frameworks such as the General Data Protection Regulation, and growing scrutiny around AI governance. Organizations today are navigating not only cybersecurity threats, but also complex compliance mandates, labour law reforms, third-party risks, and heightened stakeholder expectations.

At Riskpro, we see risk management not as a reactive function, but as a strategic enabler. Whether it is strengthening information security frameworks, building privacy programs aligned with global standards, preparing for SOC audits, or embedding governance into operational culture, resilience is now a board-level priority.

This edition brings together perspectives on:

- The evolving landscape of data protection and DPDPA readiness
- AI governance and emerging regulatory oversight
- Labour law compliance in a digitized workplace
- CISO and compliance leader insights on 2026 risk priorities
- Practical approaches to building sustainable risk frameworks

Our goal with this magazine is simple: to provide clarity in complexity. We aim to equip leaders, compliance professionals, and decision-makers with insights that are practical, forward-looking, and grounded in real-world implementation experience.

I extend my sincere gratitude to our contributors, partners, clients, and the entire Riskpro team whose dedication continues to drive meaningful impact. Your commitment to strengthening governance and protecting trust inspires the work we do every day.

As risks evolve, so must we. Let this edition serve not just as a reflection of where we stand but as a guide to where we are headed.

Warm regards,
Abigail Crasto
Editor – Riskpro Magazine
Risk Management & Privacy Advisory



DPDP ACT IN PRACTICE: FROM LEGAL TEXT TO OPERATIONAL REALITY

-SONAKSHI SINHA

The compliance deadline for the Digital Personal Data Protection Act, 2023 (DPDPA) is May 13, 2027. Many organizations are now evaluating how the law applies to their business operations. Let us see some operationality issues and a certain frequently missed compliances in most of the organisation plays both the role as a controller and a processor so every organisation in India by default will be required to implement all the measures as a Data controllers obligations.

Start with Data Inventory and Data Flows

Organizations must first understand what personal data they collect, where it is stored, and who processes it. A proper data inventory helps identify all internal systems and external partners that handle personal data. Some times In the data inventory you identify that you have large volume of data, you will identify as a significant data fiduciary, Data breach response identifying where the data was exposed, Data principal rights – deleting or correcting data across systems, Regulatory accountability – knowing which vendors or processors hold the data, This processing involves this data and regulated by IT law so we need to store for this period

Example – Retail Data Flow

In a retail environment, a single customer transaction may distribute personal data across multiple entities: POS System – billing details, phone number, purchase history, Payment Aggregator – transaction authentication, Cloud Service Provider – POS

data hosting, Logistics Partner – delivery address and contact details, Marketing/CRM Platform – loyalty programs and campaigns

Consent Management

The Digital Personal Data Protection Act, 2023 (DPDPA) is fundamentally consent-centric. Once an organization has identified its processes and the personal data involved, it must ensure that valid consent is collected for each specific purpose of data processing.

Consent should be: Clearly obtained from the data principal, Recorded and stored as evidence, easily retrievable for audits or regulatory requirements, Updated or withdrawn when the data principal changes their preference. Any change in consent status must immediately reflect across systems, business processes, and manual operations.

Organizations should also designate a responsible member or team within the project or division to regularly monitor consent management. This role ensures that any updates are properly communicated and implemented across the entire data ecosystem, including: internal teams and employees, vendors and service providers, sister concerns or group entities, third-party processors, including those operating in other countries

An alternative approach is implementing a Consent Management Platform (CMP) that helps organizations capture, track, update, and manage user consents centrally, ensuring better visibility and compliance across systems. Without a dedicated team or a tool, it is difficult for its compliance

Supply Chain Landscape

In a typical retail ecosystem, much of the supply chain may be slow to adopt privacy compliance because the retailer is usually seen as the primary data owner or Data Fiduciary under the Digital Personal Data Protection Act, 2023. However, personal data

often flows to multiple vendors such as logistics partners, marketing platforms, payment processors, and cloud providers. It is therefore critical for organizations to ensure that vendors provide the same level of data protection as the organization itself. This responsibility is usually enforced through contracts and supply chain audits. Ideally, vendors should sign a Data Protection Agreement (DPA) that clearly defines responsibilities for handling personal data. In practice, however, legal teams may find it challenging to execute lengthy standalone agreements, especially with smaller vendors or those operating in third countries who question the need for such compliance. A practical approach is to embed data protection and privacy obligations directly into the primary vendor contract as mandatory clauses, clearly specifying the roles of each party (Data Fiduciary or Data Processor), applicable compliance requirements, and audit rights. Organizations should avoid assuming vendor responsibilities and instead ensure that roles, obligations, and compliance expectations are properly documented and periodically audited across the vendor ecosystem.

Governance

Appointing a Data Protection Officer (DPO) is a key requirement under most data protection laws. An individual should be designated to oversee compliance, ensuring there is no conflict of interest in performing this responsibility. The DPO's role should not function in isolation or move in a separate direction; instead, the DPO should work closely with the Chief Information Security Officer (CISO) to gain a clear understanding of the organization's security posture and ensure alignment between privacy and security practices. Depending on the size and structure of the organization, the DPO may either personally conduct privacy audits or establish a team to carry them out. These audits should assess whether core privacy principles are being upheld, including data minimization, purpose limitation, storage

limitation, transparency, accuracy, accountability, confidentiality, and security.

Regardless of the approach, the DPO should maintain regular engagement with department heads and project leads to identify and evaluate privacy risks. The DPO should also be responsible for reviewing, deciding upon, and formally approving any residual risks associated with data processing activities.

Appropriate policies, procedures, and governance mechanisms should then be implemented to manage those risks responsibly.

Preparing for compliance with the Digital Personal Data Protection Act, 2023 should not be treated as a one-time exercise. Instead, it should be viewed as a continuous process that evolves alongside the organization's operations, technologies, and business models. Organizations that begin with foundational steps such as data inventory creation, consent management, vendor oversight, and governance frameworks can gradually build a mature privacy program within 18 months

How Riskpro Can Support

Organizations navigating the requirements of the Digital Personal Data Protection Act, 2023 often benefit from structured guidance and implementation support. Riskpro provides end-to-end assistance to help organizations operationalize privacy compliance across their processes and systems. This support includes establishing data inventories, mapping data flows, implementing consent management frameworks, reviewing vendor privacy obligations, and strengthening governance structures.

In addition to advisory support, Riskpro provides tools and structured compliance assessments that help organizations evaluate their current privacy posture. As part of this process, organizations receive a

comprehensive compliance report highlighting existing gaps, potential risks, and recommended improvements. This report can serve as a practical roadmap for strengthening privacy practices and progressively moving toward full compliance with the regulatory requirements.





DPDPA & GLOBAL PRIVACY LAWS: WHERE INDIA ALIGNS AND WHERE IT DIFFERS

-SONAKSHI SINHA

In the digital economy, personal data has become one of the most valuable assets for organizations and governments. With billions of people sharing information online through social media, e-commerce, and digital services, protecting personal data has become a global regulatory priority. Countries across the world have introduced data protection laws to safeguard privacy and regulate how organizations collect, process, and store personal information. India joined this global movement with the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act).

While India's law draws inspiration from international frameworks such as the General Data Protection Regulation (GDPR) and other global privacy laws, it also introduces unique features tailored to India's digital ecosystem. Understanding where the DPDP Act aligns with global privacy regimes and where it differs provides valuable insight into the evolving landscape of data protection.

The Emergence of India's Data Privacy Framework

India's DPDP Act, enacted in August 2023, establishes a legal framework to regulate the processing of digital personal data while balancing individual privacy rights with the need for economic growth and technological innovation. The law governs the collection, processing, storage, and transfer of digital personal data and applies both to organizations operating within India and those processing data related to individuals in India.

The DPDP Act reflects the growing recognition that privacy is a fundamental right in the digital era. As India's internet user base approaches one billion people, the need for robust data governance has become essential

to maintain trust in digital platforms and services.

Areas Where India Aligns with Global Privacy Laws

1. Recognition of Individual Data Rights

A major area of alignment between the DPDP Act and global privacy frameworks such as the GDPR is the recognition of rights for individuals over their personal data. The DPDP Act grants individuals referred to as Data Principals rights, such as:

- the right to access personal data,
- the right to correction and erasure,
- the right to grievance redressal,
- and the right to withdraw consent.

These rights mirror similar protections available under global regulations like GDPR, which emphasize empowering individuals to control how their personal information is used.

2. Accountability of Organizations

The DPDP Act introduces the concept of a Data Fiduciary, similar to the “data controller” under GDPR. Data fiduciaries are responsible for ensuring that personal data is processed lawfully, securely, and for specified purposes. Organizations must also implement safeguards to protect data and notify authorities in case of data breaches.

This emphasis on accountability reflects a broader global trend toward stronger corporate responsibility in data governance.

3. Transparency and Notice Requirements

Like most modern privacy laws, the DPDP Act requires organizations to provide a clear privacy notice whenever personal data is collected. The notice must explain what data is being collected, the purpose of processing, and how individuals can exercise their rights. Transparency is a core principle across global privacy regimes and forms the foundation of trust between individuals and organizations.

Key Differences Between the DPDP Act and Global Privacy Laws

Despite these similarities, India’s DPDP Act also differs from global privacy frameworks in several important ways.

1. Scope Limited to Digital Personal Data

One of the most notable differences is the scope of the DPDP Act. Unlike the GDPR, which applies to both digital and certain forms of structured offline data, the DPDP Act focuses primarily on digital personal data, including offline data that is subsequently digitized.

This reflects India’s policy focus on regulating data within the rapidly expanding digital economy.

2. Strong Reliance on Consent

Another distinguishing feature is the central role of consent in India’s law. The DPDP Act primarily relies on consent as the legal basis for processing personal data, whereas the GDPR recognizes multiple lawful bases such as contractual necessity, legitimate interest, and legal obligation.

This consent-centric model simplifies compliance but also places greater emphasis on clear communication and informed decision-making by individuals.

3. Differences in Sensitive Data Classification

Global frameworks like GDPR categorize certain types of information, such as health data, biometric data, or religious beliefs, as “special categories” that require additional safeguards. By contrast, the DPDP Act does not create detailed classifications for sensitive personal data and instead applies uniform protection standards to all personal data.

While this approach simplifies regulatory obligations, critics argue that it may not adequately address the unique risks associated with highly sensitive information.

4. Government Exemptions

Another key difference lies in the treatment of government access to data. The DPDP Act allows the government to exempt certain agencies from compliance requirements in specific situations, such as national security or public order.

This provision has sparked debate among privacy experts regarding the balance between individual rights and state interests.

India's Unique Approach to Data Protection

The DPDP Act also introduces concepts that reflect India's policy priorities. For example, the law establishes the Data Protection Board of India to adjudicate complaints and enforce compliance. Additionally, the framework emphasizes digital innovation and economic growth, aiming to create a balanced regulatory environment that protects privacy while enabling the growth of India's digital economy.

India's approach demonstrates an effort to create a pragmatic and flexible regulatory model that aligns with global standards while addressing domestic realities.

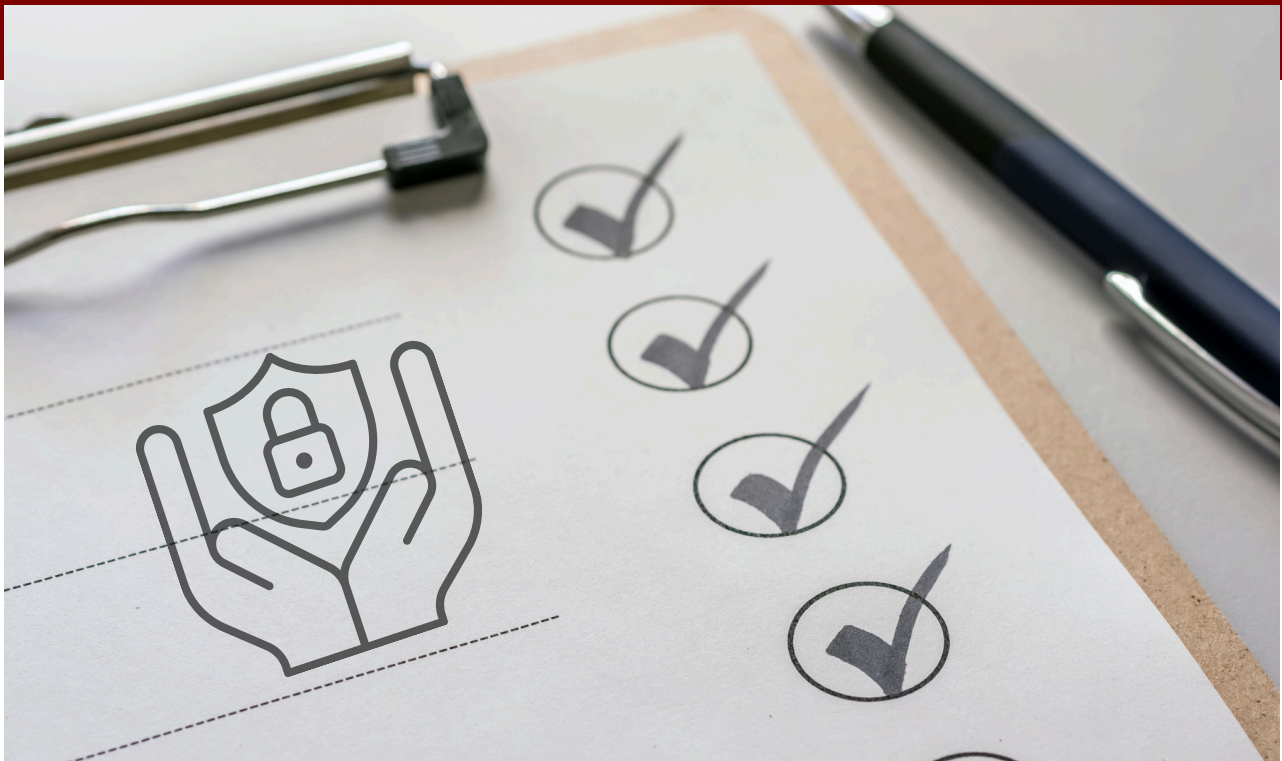
The Future of Data Privacy in India

The introduction of the DPDP Act marks a significant milestone in India's data protection journey. By aligning with international principles such as transparency, accountability, and user rights, India has positioned itself within the global privacy governance landscape. At the same time, the Act's distinctive features reflect India's unique regulatory priorities and socio-economic context.

As organizations adapt to this new framework and additional rules continue to evolve, the

DPDP Act is expected to play a crucial role in shaping the future of digital trust in India. For businesses operating globally, understanding the similarities and differences between India's privacy regime and international frameworks will be essential for building compliant and responsible data governance strategies.





DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT: A PRACTICAL COMPLIANCE READINESS CHECKLIST

-ANURAG RAJPUT

The rapid growth of digital services has significantly increased the volume of personal data collected and processed by organizations. From online platforms and mobile applications to enterprise systems and employee databases, personal data has become a critical asset for businesses. However, the increasing

reliance on personal data also raises concerns regarding privacy, misuse, and unauthorized access. To address these concerns, India introduced the Digital Personal Data Protection Act, 2023, which establishes a legal framework for the processing of personal data and defines obligations for organizations handling such information.

The Act places significant responsibility on organizations, referred to as Data Fiduciaries, to ensure that personal data is processed in a lawful, fair, and secure manner. In this context, a DPDP compliance readiness checklist helps organizations evaluate whether their policies, procedures, and technical safeguards align with the requirements of the Act. Conducting such an assessment enables organizations to identify compliance gaps and implement necessary controls before regulatory scrutiny or enforcement actions arise.

Understanding DPDP Compliance Readiness

Compliance readiness refers to the preparedness of an organization to comply with legal and regulatory requirements related to data protection. Under the Digital Personal Data Protection Act, organizations must ensure that personal data is processed only for lawful purposes, appropriate consent mechanisms are implemented, and adequate safeguards are in place to protect the data. A structured readiness checklist assists organizations in systematically evaluating their compliance posture and strengthening governance around personal data processing.

DPDP Compliance Readiness Checklist

The following checklist outlines key areas that organizations should evaluate to ensure readiness for compliance with the Digital Personal Data Protection Act.

1. Understanding and Documenting Your Data Landscape

Compliance begins with developing a clear picture of the personal data your organization handles. This involves mapping all categories of personal data collected across departments, understanding how it flows through systems, and identifying where it is stored and for how long. Organizations should also establish a detailed record of processing activities, including the involvement of employees and third-party processors. Creating this foundation helps eliminate blind spots and ensures that subsequent compliance actions are grounded in an accurate view of operations.

2. Strengthening Consent Practices

The DPDP Act places significant emphasis on valid, informed, and unambiguous consent. Compliance requires organizations to craft consent requests in clear, plain language and present them before or at the point of data collection. Individuals must be able to withdraw their consent as easily as they give it, which means providing intuitive mechanisms for revocation. Maintaining

comprehensive records of consent for both granted and withdrawn is also essential. Such practices uphold transparency and empower individuals to control the use of their personal data.

3. Building Transparent Privacy Communications

A well-designed privacy notice serves as the organization's primary communication channel with Data Principals. It must clearly explain what data is being collected, why it is needed, how long it will be retained, and who it may be shared with. Instructions on how individuals can exercise their rights and file grievances with the relevant authority should also be included. Ensuring that privacy notices are not only compliant but also easily understandable builds trust and strengthens accountability.

4. Enabling Rights of Data Principals

Organizations must establish efficient internal mechanisms to respond to requests from Data Principals. These include the right to access personal data, correct inaccuracies, request deletion when the original purpose is fulfilled or consent is withdrawn, and lodge grievances. Data Principals can nominate another individual who may exercise these rights on their behalf in the event of death or incapacity. The Act mandates timely responses, which means organizations need organized processes supported by well-trained staff. Enabling these rights demonstrates a commitment to fairness and respect for individual autonomy.

5. Modernizing Security and Protection Safeguards

Compliance demands the adoption of strong organizational and technical safeguards. This includes implementing encryption, managing access controls, and conducting regular security audits and vulnerability assessments. The goal is to minimize the risk of unauthorized access, data breaches, and misuse. Ensuring secure transmission,

storage, and disposal of data reflects a proactive approach to risk mitigation and demonstrates due diligence under the Act.

6.Preparing for Data Breach Response

A comprehensive breach response plan is a critical compliance requirement. Organizations must be able to promptly detect, assess, and respond to incidents. A documented breach notification procedure should outline how and when the Data Protection Board and affected individuals will be informed. Completing root-cause analyses and implementing corrective actions are essential steps in preventing recurrence and demonstrating accountability.

7.Aligning Data Retention and Destruction Practices

The DPDP Act enforces the principle that personal data should be retained only as long as it is necessary for the stated purpose. Organizations must define structured retention schedules for different categories of data and ensure secure destruction or anonymization once the purpose is fulfilled. Effective retention management reduces risk, frees storage resources, and supports the principle of data minimization.

8.Managing Third-Party Processors

Since many business operations involve outsourced solutions or service partners, organizations must ensure that all third-party entities follow the same data protection standards. Contracts should be updated to reflect DPDP-aligned obligations, and periodic assessments must be conducted to verify compliance. Maintaining an updated inventory of all processors and understanding the nature of data shared with them is essential.

9.Establishing Governance and Accountability Structures

Good governance requires designating internal roles and responsibilities for data protection. Significant Data Fiduciaries may need to appoint a Data Protection Officer (

DPO) to oversee compliance, coordinate grievance redressal, and implement privacy frameworks. Clear role definitions ensure smoother operations and consistent adherence to policies. Developing and maintaining comprehensive data protection policies further reinforces accountability.

10.Fostering Employee Awareness and Training

Human awareness remains one of the strongest defences against data-related risks. Organizations must conduct regular training sessions for employees on the DPDP Act, internal data protection policies, and breach detection procedures. Training should be mandatory for new hires and refreshed periodically, especially after any data-related incident. Such initiatives help build a culture of privacy and responsibility across the organization.

Conclusion

DPDP compliance is not a one-time project but an evolving journey that requires ongoing vigilance, improvement, and commitment. By strengthening consent practices, enhancing transparency, enabling individual rights, securing data, and fostering a culture of accountability, organizations can transform regulatory compliance into a meaningful competitive advantage. Organizations that fail to comply with the provisions of the DPDP Act, 2023 may face significant financial penalties, with fines reaching up to INR 250 crore for certain violations, depending on the nature and severity of non-compliance. Early preparation therefore ensures not only legal conformity but also protects organizations from regulatory penalties and strengthens their reputation in an increasingly privacy conscious digital economy.



AI RISK AND RISK FROM AI

-CASPER ABRAHAM

There are 2 broad streams of risk around AI. "AI risk" and "Risk from AI". So, what's the difference?

AI risk is the inherent risk from AI itself. Creators of risk. Thus far with IT, choice of technology, architecture, partner or startup, computing, data, automation in fact everything you know about IT is about repeatability, reliability and once tested will give you the same result every single time. Once tested and proven you could trust IT (More or less). If AI is an IT discipline, it now introduces variability and probability of a magnitude between 0 and 1. Especially with Deep Learning, GenAI, AGI etc. With the introduction of any form of AI, you introduce hallucination, blue ocean thinking vs red, green world vs red world debate, opinions and everything is right and correct - it only depends on your perspective.

All the above before you even get to "Risk from AI". Users of risk. Recipients. Affected. What are you planning? Where is your data? Where is the rest of the data coming from? Who has it? Who owns it? What are vested interests in the data? Which industry? What application? What about privacy? What about copyright and ownership? How much are you going to rely on the output of your inputs depending on the AI? Will AI use discretion in the output given to you? Are the inputs in text, images, audio or video media? Are the outputs in the same media as the inputs? If converted from one media to another the anecdote that comes first in mind is "Lost in Translation". Can you afford the loss in Translation? Can you ever quantify and qualitatively decide on anything that comes out with an AI layer on top of it?

Two key threats to perhaps even humanity at large is "mass surveillance" and "autonomous weapons". You (as an individual), as a community, group or voting block, or enterprise is going to be either an "insider" or an "outsider" to this. AI Risk vs Risk from AI. If you follow the money these 2 have enormous possible public and private floats. If everyone

in a country wants low-cost healthcare all health data has to be more or less public and a national asset. Something like what India is attempting and the UK has as NHS. If you don't want your soldiers killed during a war or defending yourself, go "autonomous". Embed all your weapons with AI. But whose AI? Which ones are going to give it to you? Are their back-door viruses, hacking, human controls? Related concerns could fill many books leave alone one article. In a country like China with a single-party rule imagine if policing, propaganda and surveillance is enhanced by AI and automated. China can export this whole eco-system to other world wannabe dictators. Would any society of humans put up with it? For how long?

One aspect of all the hype is the future of Technology, IT and ICT (Information & Communications Technology) is AI. Any and all legacy software, ERP's, SCMs, CRM's and all the other 3 letter acronyms will shift toward AI. So, you will be hearing a lot of the same hype and click-baits, however with minimal substance. 99 out 100 startups, especially in AI are going to fail. Today's news won't even exist a year later.

Your "data-set" is the "new oil". The protection of "your data-set", first distinguishing what is yours and what is not and then protecting it, leveraging it, monetizing it while minimizing risk is and will be the essence of any business. Ofcourse you are going to use public and private paid-for data-sets, however the key for you is to be able distinguish this as any information or insight you gather in the course of doing your business with AI. In a way it's similar to your original thoughts, creativity, innovation, copyright and the expression of a copyright in human intelligence – now you (and the world is grappling with it) have to find a way to control your AI expression of it.

Now let's take, another aspect of AI, nature and natural selection. Nature over millions of years has shown biases. Arguable biases can

include; survival of the fittest, winner takes all, the weak are sacrificed for the benefit of the group, flowers are weeds with a large advertising budget, a crying baby gets more milk for humans means the tallest trees, the brighter flowers, the louder, shriller mating calls all have "bias" implications. Won't all these biases have to be a part of the AI data-set? Now think up a list of all the risks each of these will introduce into anything you do with anything you claim to have AI on it.

Another risk aspect of AI is that it is all encompassing. All the facts, data & information in written text form, graphics, spoken word, videos, physical footage on magnetic tape, audio tapes. All of history, science and artworks. Sculpture, archaeology, education, healthcare, manufacturing, travel, tourism, hospitality ... it is a part of or affects, is changing and will change every action of humans and humankind.

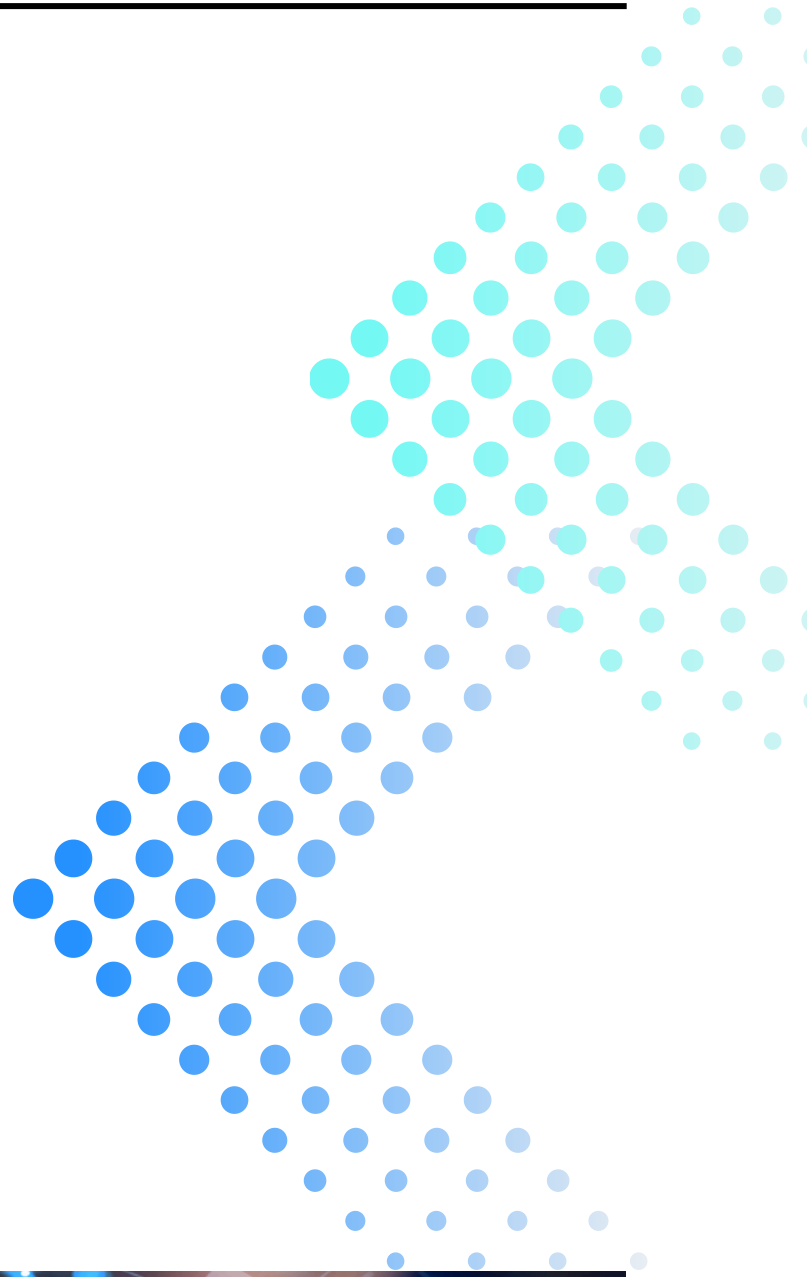
My advice to you, don't put "AI" on any of your labels, till you really understand what "AI risk" and "Risk from AI" can do to your business, your customers, your vendors, your colleagues, your communities and your products. Just like "greenwashing" where just using the colour "green" in your logo and all your communications you fool the receiver into thinking you are climate friendly – "AI washing" is identical. My pressure cooker is AI – it whistles when the pressure inside is high. My battery is AI – it knows it's run out of juice and packs up. My teeth are AI – it hurts when it knows it can't take it anymore. By the way; forget Governments and Regulators, they will be hard pressed to keep up with anything like the juggernaut that AI has released - they can't, won't and should not be saving you anyway. It's like stating that the long-term solution for people on earth is to move to another planet. Yes, it's a solution - but not realistic and definitely not in our life time. We have to learn to live and let live. The best way is to understand and manage risk.

While setting goals like safe AI, trusted AI, and

AI resilience we have to do the basics and escalate the small threats before they become larger threats.

Conclusion

Traditional risk management tells you to focus on only what you can control and on the downside of risk. Risk registers, likelihood, impact and mitigation are centered around these 2 core concepts. I would suggest that given the increase of even black-swan events, and the un-foreseeable nature of AI that we all approach it as a global common “risk register” and view the applicability of this ‘date-set” to your enterprise as an individual, group, community, vertical sector or horizontal function. In parallel consider the “opportunity and upside” possible with AI. It’s time to consider risk holistically as “Integrate Risk Management” and not just GRC, ERM, ESG, Trusted AI. We at Riskpro can partner with any firm of any size globally when you talk to us.





ARTIFICIAL INTELLIGENCE – REGULATORY ENVIRONMENT

-SUCHETA UPENDRA

As Artificial Intelligence (AI)-based systems become a norm than an exception, governments around the world are introducing regulatory frameworks to ensure that AI is developed and used responsibly.

These regulations focus on managing risks such as threat to safety and security, bias, privacy, misinformation, and societal impacts. Some of the key regulations already in effect are listed below.

European Union: Regulatory bodies in European Union have always been trendsetters and introduced first comprehensive EU Artificial Intelligence Act to govern AI. It establishes a risk-

based approach that classifies AI-systems into different categories based on the risk classification such as Prohibited AI-systems (Unacceptable risk), High-risk, Limited risk, and Minimal risk. Compliance obligations differ based on the category.

- **United States:** Similar to the approach used for Data Privacy, the USA adopted approach of state and sectors-specific regulations :

New York City's local law is among the first to protect job applicants from AI-bias – a common problem impacting automated employment decision tools (**AEDT**) used for hiring and promotions. It mandates an independent race/gender bias audits on AEDTs and public disclosures of audit results. It also requires advance notification to candidates about using AEDTs for hiring process.

Colorado's AI Act requires a developer of a high-risk artificial intelligence system (high-risk system) to use reasonable care to protect consumers from any known or reasonably

foreseeable risks of algorithmic discrimination in the high-risk system. A person doing business in this state, including a deployer or other developer, that deploys or makes available an artificial intelligence system that is intended to interact with consumers must ensure disclosure to each consumer who interacts with the artificial intelligence system that the consumer is interacting with an artificial intelligence system.

- India strengthened its approach to regulate AI generated contents and deepfakes through amendment to Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These amendments introduce specific obligations for digital platforms, AI providers, and users to curb misuse of synthetic media such as deepfake videos, synthetic audio, and AI-generated images.

Conclusion

AI regulations worldwide are evolving rapidly with different countries using different approaches.

To ensure compliance with growing number of obligations, organizations should proactively take the following steps:

- Establish AI-Governance framework for developing and using AI-based systems
- Conduct risk assessment for AI systems used within the organization and developed by the organization.
- Train it's team in responsible development and use of Artificial Intelligence.
- Deploy technical detection (e.g. detection of deepfakes) and monitoring controls as applicable to the organization's context

Additionally, organizations may also consider controls and guidance provided by various frameworks such as ISO/IEC 42001, Responsible AI Framework, and NIST AI risk management framework to ensure implementation of robust AI Governance framework and technical controls.





CYBER RISK IN 2026: WHY PREVENTION ALONE IS NO LONGER ENOUGH

-SIDHARTHA SHARMA

The Vanishing Perimeter & the Shadow AI Problem

The modern enterprise has no perimeter. Cloud adoption, SaaS sprawl, remote work, and API, driven ecosystems have dissolved the boundaries that once defined "inside" and "outside." Attackers no longer break in, they log in.

Nearly 80% of successful attacks today are malware, free, relying on stolen credentials, identity abuse, and legitimate system access. No alarms, no malicious files; just a silent intrusion through trusted pathways.

The uncomfortable truth: the security industry's decades, long focus on prevention has hit a structural ceiling. In 2026, the organizations that survive are not those with the highest walls, they are those that recover the fastest.

Modern enterprises operate sprawling digital ecosystems: hundreds of SaaS applications, thousands of API connections, blended IT/OT environments, and a rapidly expanding layer of unsanctioned "Shadow AI."

Employees and teams are quietly deploying AI tools outside formal governance: processing sensitive data through systems security teams neither control nor monitor. Each connection is a doorway; each integration, a potential pivot point.

The Next Wave of AI, Enabled Threats

Agentic AI attacks, autonomous systems executing multi, step breaches without human direction

Deepfake fraud, executives and staff impersonated via cloned voice and video
AI generated vulnerabilities, insecure "vibe coded" software deployed silently into production

Shifting from "Prevent at All Costs" to "Survive and Recover"

Cybersecurity in 2026 is fundamentally a risk management discipline, not a prevention exercise. Breaches will happen. The measure of an organization is how quickly it absorbs the impact and restores normal operations with minimal lasting damage.

The Four Pillars of Cyber Resilience:

1. Governance & Board Accountability

Translate cyber risk into financial and operational language the board can act on. Tie resilience metrics to executive accountability.

2. Operational Readiness & Rehearsed Response

Incidents cannot be improvised. Conduct regular tabletop drills involving legal, communications, and operations not just the security team. The organizations that recovered fastest from 2025's major attacks had rehearsed their response before the crisis hit.

3. Technology Engineered for Recovery

Immutable backups, Zero Trust architecture, and network segmentation ensure survivability when prevention fails. Design for recovery, not just detection. Assume the internal network is already compromised.

4. Human Resilience in a Deepfake World

Employees must operate knowing that emails, voices, and video calls can be fabricated. Continuous behavioral training and out of band verification protocols are non-negotiable in an era of AI generated impersonation.

The Integrated Security Imperative

Risk Advisory defines what matters most. Virtual CISO leadership defines how to secure it. Continuous pen-testing proves whether controls work. Compliance frameworks ensure it is sustainable and auditable.

Together, these form a closed loop security program that continuously adapts to threat evolution not a set of disconnected tools purchased in response to the last incident.

Organizations in 2026 will be judged not on whether they were breached, but, on how well they withstood it.

The Road Ahead

The organizations that will thrive in 2026 and beyond are not those with the strongest defenses—but those with the greatest adaptability.

They will:

- Quantify cyber risk in business terms
- Continuously monitor third-party ecosystems
- Govern AI with discipline
- Automate detection and response
- Align security with business resilience

The Convergence: A Unified Security Program

The real power emerges when these elements are integrated:

- Risk Advisory defines what matters most
- vCISO leadership defines how to secure it
- Pen-testing & continuous validation prove whether it works
- Compliance frameworks ensure it is sustainable and auditable

Final Imperative

Organizations in 2026 face a simple but unforgiving truth:

You will be tested—not just on your ability to prevent attacks, but on your ability to withstand and recover from them.

Risk advisory, virtual CISO leadership, continuous testing, and strong compliance are not independent services. They are **interdependent pillars of cyber resilience.**



THIRD-PARTY RISK: THE HIDDEN COMPLIANCE MULTIPLIER

-SANKET PRABHU

In today's interconnected economy, no organization operates alone. Vendors manage our data, suppliers power our production, consultants influence strategy, and cloud providers host our most sensitive information. These partnerships enable scale and efficiency but they also introduce a powerful and often underestimated force in compliance: third-party risk.

Too often, compliance is viewed as a contained, internal function. Policies are drafted, controls are implemented, audits are performed, and leadership assumes the risk perimeter stops at the corporate boundary. In reality, that boundary is porous. Third parties

act as extensions of the enterprise, and with every outsourced service or strategic partnership, the organization's compliance exposure expands.

This is why third-party risk is best understood as a compliance multiplier.

Why It's a Multiplier, Not Just an Add-On:

Third-party risk does not increase compliance complexity in a straight line. It multiplies it.

Consider a company operating in three countries. Internally, it already manages data privacy requirements, anti-corruption controls, financial reporting obligations, and cybersecurity standards. Now introduce external partners: a cloud hosting provider, a payroll processor, a marketing agency handling customer data, and a logistics partner operating in emerging markets.

Each third party introduces its own risk profile different geographies, subcontractors, technologies, and regulatory obligations. These risks intersect with the organization's

own controls, creating a web of dependencies. A weakness in one link can expose the entire system.

This interconnectedness creates compounding exposure. A cybersecurity vulnerability at a vendor can lead to regulatory investigations, litigation, operational disruption, and reputational harm all stemming from a risk outside the company's direct control.

That is the multiplier effect in action.

The Limits of Checkbox Compliance

Historically, many organizations approached third-party risk management as a procurement exercise. Vendors completed questionnaires, signed compliance representations, and provided certifications. Files were stored. Contracts were executed. Business moved on.

But static due diligence cannot keep pace with dynamic risk.

Cyber threats evolve continuously. Sanctions lists change overnight. Data protection enforcement intensifies year by year. Environmental and social governance expectations shift with investor pressure and public awareness. A one-time onboarding review does little to address ongoing exposure.

Regulators increasingly expect continuous oversight. This includes risk-based vendor segmentation, periodic reassessments, contractual audit rights, cybersecurity monitoring, and documented escalation processes.

Effective third-party risk management is no longer a formality it is an ongoing governance discipline.

Reputation: The Invisible Cost

While regulatory penalties are significant, reputational damage often carries the deeper impact. In a hyper-connected world, third-party failures can become public crises within hours.

Customers rarely distinguish between a company and its supplier. Investors do not pause to examine subcontractor arrangements before reacting to allegations of misconduct. A data breach at a vendor can erode trust built over decades. A supplier's environmental violation can undermine carefully cultivated ESG positioning.

Reputation amplifies third-party risk beyond regulatory consequences. It transforms operational missteps into brand-level crises. For many organizations, the true cost of inadequate oversight is not measured in fines but in lost confidence.

Preparing for the Next Wave

As digital transformation accelerates, third-party ecosystems are becoming even more complex. Artificial intelligence vendors, cross-border fintech providers, outsourced analytics firms, and global data processors are now integral to business models.

Each innovation introduces new regulatory questions and new layers of dependency.

Organizations that invest now in scalable, risk-based third-party governance frameworks will be better positioned to adapt. Those that rely on outdated, reactive models will struggle to maintain visibility as their ecosystems expand.

The future belongs to companies that recognize that they do not operate alone and plan accordingly.

Conclusion

Third-party risk is not hidden because it is minor. It is hidden because it is embedded woven into supply chains, contracts, APIs, and operational workflows. Every partnership carries compliance implications, whether acknowledged or not.

As regulatory expectations tighten and stakeholder scrutiny intensifies, organizations can no longer afford to treat third-party oversight as an administrative afterthought. It is a multiplier capable of amplifying both weakness and strength.

Managed poorly, it expands exposure across legal, operational, and reputational dimensions. Managed well, it becomes a foundation for resilience, credibility, and sustainable growth.

In a world defined by interconnectedness, effective third-party risk management is no longer optional. It is the quiet engine of modern compliance.





GEO-POLITICAL RISK

-LAXMIKANT GUPTA

Geo-Political Events, Geo-Political Risk has been a buzz word in last few years whenever there is any economic turmoil or war like situation with any country or region. With globalisation of economy and opening of avenues for Indian Companies globally, overall economy is more exposed to outside circumstances.

From the perspective of Operational & Strategy risk management, this is recognised as follows:

- It is an important Emerging risk as Operational Risk has evolved upto a certain extent due to regulatory push like BASEL norms, Central Bank guidelines etc.
- It is an external risk majorly coming due to the external risk factor, or geopolitical or economy or war like situation in any region or countries.

Eg – economic crises – Greece crises 2012.

Asian crises in 1997, Venezuela's decade long petro and currency crisis, Egypt's 50% depreciating currency followed by 17-20% inflation, Recent Bangladesh and Shri Lanka crises, Russia – Ukraine war etc.

Indicators of Geopolitics risk exposure :

The basic indicator of geopolitics risk is

- 1.Foreign exchange rate becomes volatile and starts move in one direction, mostly with depreciation in emerging countries' currency values
- 2.Oil price becomes volatile and mostly it increases

Other indicators of increased geopolitical risks are :

Supply chain issues, blocking either the geographical route or increasing supply restrictions, which may be due to relationship between two countries or supply shortages / deficit supplies in supplying countries. Example is Rare Earth Material like Scandium, Yttrium etc. which affects EV batteries. Semi-Conductors are such other supply chain issues which may be due to reasons like Red Sea disruptions

also.

- Increasing countries' import bill, adverse current account and balance of payment position which all may lead to inflation in costs and depreciating currency.

Locally, Geo-Political crisis may be reflected by :

- Election year policies where Government may take recourse to Essential Commodities Act to combat inflation, increase subsidies, reduce exports and stock holding limits for sensitive crops like rice, wheat, chana, pulses, sugar, increased subsidies etc.
- In case of monsoon shortfall, the above measures may be more aggressive while in case of surplus monsoon, focus may be on increasing subsidies and minimum support price of crops.
- The above inflationary situation specially in sensitive commodities may affect APMCs and commodity derivatives markets as well. Sugar to use of ethanol in petroleum products and other Boards like Spices Board, Tea Board etc may have their own policies affecting the profitability of their producers and users.
- On IT side, policies on data centres, holding of data cross-border or within the country, data sovereignty and cross-border transfer are a few examples of geo-political factors.
- Other policies like Make in India, China +1, FDI, Export control and supply chain sanctions,

Other indicators are due to secondary impacts and depends upon country-to-country including aspects of,

- Countries of your imports
- Countries of your exports of goods, labour, white collar professionals, outsourcing to India
- Competing countries to increase your supplies or your markets. For e.g.

- Bangladesh crisis led to surge of textile industry in India at Tirupur, Ludhiana, Cotton belt, as Bangladesh textile exports reduced.
- Countries where you have projects, capex. For e.g. construction and energy projects in Middle East affects various companies in India as their investment in capex is at stake.

How to manage this Risk

1. Geo political risks can be better managed by labour intensive companies as labour can be moved out. However, it cannot be done with factories and plants located abroad.
2. Keeping an eye on economies of exporting and importing countries
3. Keeping an eye on their equation with other countries including competing countries
4. Keep an eye on substitute products and countries from where substitute materials can be supplied
5. Keep an eye on overall world equation across nations. A trade war between two countries neither of which is your own can still reshape your supply chain. The US-China tariff battles, for example, rerouted entire industries through Southeast Asia.
6. Strategy to make import substitute product
7. Enhancing domestic sales Export-led growth is powerful, but fragile. The businesses that weather geopolitical storms best are those that can fall back on home demand when foreign markets seize.
8. Board should have diversity of skills. Board should have more frequent meetings to discuss geo-political events

Stress Testing and Scenario Analysis:

Carrying out regular stress testing or scenario analysis on the overall balance sheet and future projected business will throw various lights on unforeseen Geopolitical risks. While

carrying out this, various geo-political factors can be noted. For e.g. it may be:

- Extent of production and sales of sensitive commodities like Cigarettes
- Extent of production using various sensitive materials or materials in shortage, like Paints, Sugar
- Extent of export and imports per country or region
- Extent of products largely depends servicing during foreign exposure of customers. For e.g. tours travel, hotels, education finance to students going abroad etc.

Logically, countries or regions should be identified for various categories and accordingly scenario analysis can be done. A few e.g. of scenarios may be:

- Closure of Oil supply for 2-3 months
- USD = Rs.125
- Oil = USD 125 per barrel
- 10% appreciation in currency of countries from where imports are done + reduced Elasticity of local demand
- 10% depreciation in currency of countries to which exports are done + increased elasticity or competition or substitutes with foreign buyers
- Extent of foreign technology used to include, IT software and tools, and borderless connection. These may turn out to be stormy for the businesses.
- Frozen mobility of foreign or local professionals due to country specific policies

Such stress testing will throw light on extent of unforeseen foreign exposure and ways to tackle those. This will also highlight risk figures or risk postures on geo-political sensitivity of your company, industry and the whole nation.





KEY REGULATORY & RISK TRENDS TO WATCH IN 2026

-CASPER ABRAHAM

Pre-amble

While the trend in the US is less regulation especially around Climate risks and AI the rest of the world continues to grapple with these 2 enormous challenges. How to encourage innovation, scale, reach and growth while containing the inherent and obvious risks from these 2 key areas.

Key-risks

While there are studies, data sources and reports galore the World Economic Forum is what I see as being one of the better go-to resources. According to their 2026 outlook the 10-year horizon top-10 are ... (i) Extreme weather events (ii) Biodiversity loss and ecosystem collapse; (iii) Critical change to Earth systems; (iv) Misinformation and

disinformation; (v) Adverse outcomes of AI technologies; (vi) Natural resource shortages; (vii) Inequality; (viii) Cyber insecurity; (ix) Societal polarization; and (x) Pollution.

Their 2-year horizon – till DEC 2027 – lists ...

(i) Geoeconomic confrontation; (ii) Misinformation and disinformation; (iii) Societal polarization; (iv) Extreme weather events; (v) State-based armed conflict; (vi) Cyber insecurity; (vii) Inequality; (viii) Erosion of human rights and/or of civic freedoms; (ix) Pollution; and (x) Involuntary migration or displacement

The common thread is environment and geopolitics ignoring threat. As a root cause; migration of labour; water scarcity; food security; hoarding, hedging, leveraging of resources; nationalism and protecting markets; increase in physical and technology base armed protection of the tribe is one threat. The other common thread is Information & Communications Technology. As it evolves toward AI (Artificial Intelligence) that encompasses “business” and “social” with lower cost reach, wider and deeper

penetrations and plethora of device introduction connected by internet, mobile, internet of things, satellite communications ... big-brothers can be seen everywhere. Human rights and freedom are the push back against these 2 leading risks.

Anecdotally “data” is considered the “new oil”. While fossil-fuel based energy is transiting to renewable green energy; the protection of “your data”, first distinguishing what is yours and what is not and then protecting it, leveraging it, monetizing it while minimizing risk is and will be the essence of any business irrespective of your sector. Note – data is any information or insight you gather in the course of doing your business.

Following my conclusion – further in this article – is that you have to expand your risk portfolio and registers allowing risk appetite or risk aversion guide-lines to push-down decision making that incorporates a scientific measurable integrated risk management umbrella around your organisation perhaps even to survive, while attempting to thrive. While traditional ERM (Enterprise Risk Management) is a great start, being pro-active and trying to anticipate “risk” is an art that will stand any business or social organisation in good stead; whether in the coming 2 or 10 years.

Conclusion

Traditional risk management tells you to focus on only what you can control and on the downside of risk. I would suggest that given the increase of even black-swan events that could affect you from the 20 listed risks in this article. You should consider risks beyond your control. In parallel you should ALSO consider the upside opportunities of all business activity with a “risk” perspective. The mechanism is Risk registers, likelihood, impact, risk mitigation, authority, responsibility and accountability assignment of each risk. Each line-item should be

centered around these 2 core concepts. At an individual level, community or divisional level, enterprise, county or state and NOT limit it to national issues. It's time to consider risk holistically as “Integrate Risk Management” and not just GRC, ERM, ESG. We at Riskpro can partner with any firm of any size globally when you talk to us.





SMART RESOURCING FOR RISK & CYBERSECURITY TEAMS, PRESENTED BY RISKPRO INDIA.

-RITA SHEWAKRAMANI

This article is designed to help you understand how modern organizations are strengthening their Risk and Cybersecurity functions using flexible resourcing models like vCISO, ITGRC, Data Privacy Retainerships, Loan staffing, and Staff augmentation.

Whether you're a CXO, Risk Manager, HR leader, or a founder, the goal of this article is to give you clarity on:

- When to use each model
- The advantages and limitations
- ROI comparisons
- And how to create the right mix for your organization's maturity

What problems are companies facing today in the changing Risk and Cybersecurity Landscape

As you know IT has become pervasive across all the functions in a company. IT is the blood that runs in the body of the entire organisation. Now a days companies are grappling with Cybersecurity talent shortage, Compliance pressures, Rising cyberattacks and high costs of such personnel.

- Talent shortages & rising cyber threats
- Why traditional hiring models fall short
- Business pressure for agility (Alertness) + cost-efficiency
- Rising cyber threats & regulatory pressure
 - Cyber threats like ransomware, phishing, and advanced persistent threats continually evolve, challenging defenses.
- Budgets under pressure
- Shift to flexible, on-demand talent

Why Traditional Hiring Fails

- High cost of full-time leadership
- Difficulty finding specialized skills
- Long hiring cycles
- Skills mismatch in audit & cyber roles

How vCISO & IT GRC solve it

IT GRC Frameworks like SOC2, ISO 27001, GDPR, DPDPA, PCI DSS etc covers the following areas which requires a IT GRC experienced person or a CISO/ VCiso to deliver the same:-

- Governance
- Risk
- Compliance
- Framework alignment
- Monitoring
- Reporting

How Smart Resourcing helps

Smart Resourcing helps in Retainership and Staff augmentation for roles like Vciso, IT GRC, IT Auditor, Internal Auditor, Risk Professional, Data Privacy etc (Basically GRC personnel – IT and Non IT).

Retainership and staff augmentation are both models for outsourcing, but they differ in scope and duration.

Retainership involves a long-term, ongoing commitment where a client pays a recurring fee for access to a provider's services, often for a defined set of tasks or expertise. Eg: Vciso, DPO, GRC Advisory, Policy mgmt, Ongoing Compliance, ISO, DP etc. Deliverables are monthly and its value for SMEs & fast-growing companies.

Staff augmentation, Client hires **dedicated resources** through you to work under **client's direction and control**.

Typical Roles - GRC analysts, IT auditors, SOC analysts, Cloud security engineers, Compliance coordinators.

On the other hand, is a shorter-term solution where a client hires temporary staff to supplement their existing team, often on an hourly or project basis.

Loan staffing is short-term deployment for

peak workload. Temporary lending of internal employees to another organization for a defined period.

Roles: Audit peak periods, Compliance deadlines, Maternity cover / attrition gaps, Short-term regulatory mandates
Loan staffing offers rapid deployment of skilled cybersecurity professionals without lengthy hiring cycles.

To conclude

Many organisations don't want to hire full-time resources due to cost or uncertainty. Retainership gives predictable expert support. Staff augmentation provides skilled professionals without long-term HR overhead. Loan staffing helps during peak workload.

Why Cybersecurity Leadership Matters

- Cyber threats are increasing rapidly
- Regulations and compliance requirements are stricter
- Leadership teams lack time and security focus
- SMEs don't need a full-time CISO but they do need CISO-level guidance
- Shortage of skilled cybersecurity professionals
- Unclear governance and ownership
- Compliance efforts are scattered and reactive
- These gaps create serious business and security risks

Cyber threats are increasing rapidly

Cyberattacks are becoming more frequent, more sophisticated, and more targeted. Ransomware, data breaches, phishing, and supply-chain attacks are no longer limited to large enterprises—SMEs are equally at risk due to weaker defences and limited resources.

Regulations and compliance requirements are stricter

Governments, regulators, and customers now

expect stronger data protection and security controls. Standards like ISO 27001, SOC 2, GDPR, and industry regulations require continuous compliance—not one-time efforts—making security and governance more complex.

Leadership teams lack time and security focus

Business leaders are focused on growth, operations, and revenue. Cybersecurity often becomes a secondary priority until an incident or audit occurs. Without dedicated security leadership, risks remain unmanaged and decisions are delayed.

SMEs don't need a full-time CISO – but they do need CISO-level guidance

Most SMEs cannot justify the cost of a full-time Chief Information Security Officer. However, they still need strategic security direction, risk-based decision-making, and board-level reporting—capabilities that require senior-level expertise.

Shortage of skilled cybersecurity professionals

There is a global shortage of experienced cybersecurity talent. Hiring and retaining skilled professionals is expensive and time-consuming, leaving many organisations understaffed or reliant on junior resources without strategic oversight.

Unclear governance and ownership

Security responsibilities are often spread across IT, compliance, legal, and business teams with no clear accountability. When ownership is unclear, critical security decisions fall through the cracks and risks remain unresolved.

Compliance efforts are scattered and reactive

Many organisations approach compliance only when an audit, customer request, or incident occurs. Controls are implemented in silos,

documentation is inconsistent, and there is no unified GRC structure leading to inefficiencies and repeated work.

These gaps create serious business and security risks

Together, these challenges increase the likelihood of breaches, audit failures, financial losses, reputational damage, and regulatory penalties. Without structured governance and leadership, organisations remain reactive instead of resilient.





LABOUR COMPLIANCE AS A GOVERNANCE & ESG ISSUE

-ABIGAIL CRASTO

In boardrooms across industries, Environmental, Social, and Governance (ESG) considerations have shifted from being reputational enhancements to strategic imperatives. While environmental metrics and climate disclosures often dominate the ESG conversation, labour compliance is emerging as a core governance and social accountability issue one that directly impacts sustainability, investor confidence, and long-term enterprise value.

Labour compliance is no longer just about adhering to statutory requirements. It is about demonstrating ethical employment practices, ensuring worker dignity, mitigating

operational risk, and embedding accountability into organizational governance frameworks.

The “S” in ESG: Human Capital at the Center

The Social pillar of ESG focuses on how organizations manage relationships with employees, contractors, and communities. This includes:

- Fair wages and statutory benefits
- Safe and healthy working conditions
- Non-discrimination and equal opportunity
- Prevention of harassment and exploitation
- Transparent grievance redressal mechanisms
- Ethical supply chain labour practices

Non-compliance with labour laws whether related to wages, social security, working hours, or workplace safety can quickly escalate into regulatory action, reputational damage, and investor scrutiny.

In India, the introduction of consolidated labour codes such as the Code on Wages, 2019, Occupational Safety, Health and Working Conditions Code, 2020, Code on

Social Security, 2020, and Industrial Relations Code, 2020 reflects a structural shift toward modernized compliance and digital reporting frameworks. Organizations that fail to align with these evolving requirements face not only penalties but strategic setbacks.

Labour Compliance as a Governance Risk

Governance under ESG is about oversight, accountability, and risk management. Labour compliance intersects directly with governance in the following ways:

1. Board-Level Accountability

Regulators and investors increasingly expect boards to oversee human capital management. Failure to monitor labour compliance can expose directors to legal and fiduciary risks.

2. Internal Controls & Documentation

Payroll integrity, statutory contributions, contractor compliance, and employee classification require strong internal control systems. Weak controls may lead to financial misstatements and audit qualifications.

3. Third-Party & Supply Chain Exposure

Organizations are now being evaluated on how their vendors treat workers. Non-compliance within supply chains can result in ESG downgrades and contractual termination by global partners.

4. Litigation & Regulatory Action

Labour disputes, class actions, and inspections can disrupt operations and impact financial stability. Governance frameworks must proactively mitigate such risks.

Investor & Regulatory Expectations

Global investors increasingly evaluate ESG disclosures to assess long-term sustainability. Human capital disclosures attrition rates, workforce diversity, pay equity, training investments, and safety metrics are now part of annual reporting frameworks.

In India, the Securities and Exchange Board of India mandates Business Responsibility and Sustainability Reporting (BRSR) for listed

entities. Labour compliance metrics form a critical part of this disclosure framework.

Beyond domestic regulation, multinational organizations must also consider global standards such as the International Labour Organization conventions, UN Guiding Principles on Business and Human Rights, and supply chain due diligence requirements emerging in Europe and other jurisdictions.

Labour governance is therefore not a local compliance issue it is a global competitiveness issue.

The Cost of Non-Compliance

Failure in labour governance can lead to:

- Financial penalties and back-payment liabilities
- Project delays due to regulatory intervention
- Reputational harm amplified through social media
- Loss of investor confidence
- ESG rating downgrades
- Contract termination by global clients

In an era of transparency, employee grievances and labour violations surface quickly and publicly. The cost of remediation is often far greater than the cost of preventive compliance.

India's Labour Law Reforms: Are Organizations Truly Prepared?

In recent years, India has undertaken one of the most significant overhauls of its labour regulatory framework consolidating over 40 central statutes into four comprehensive codes. While the intent behind this reform was to simplify compliance, promote ease of doing business, and modernize labour governance, the transition has posed critical questions for organizations of all sizes: Are they truly prepared for the new regime? And can they operationalize these reforms without exposing themselves to governance risk?

Understanding the Labour Law Reforms

The Government of India has replaced multiple outdated enactments with the following four labour codes:

- Code on Wages, 2019 – Unifies laws relating to wages, bonuses, and equal remuneration.
- Industrial Relations Code, 2020 – Regulates trade unions, collective bargaining, and dispute resolution.
- Occupational Safety, Health and Working Conditions Code, 2020 – Consolidates multiple laws into a comprehensive framework for worker safety and welfare.
- Code on Social Security, 2020 – Expands social security coverage for both organized and unorganized sectors.

These codes simplify language, consolidate obligations, and emphasize digital compliance mechanisms. However, implementation timelines, state-level adaptations, and enforcement readiness vary across jurisdictions—leaving many organizations uncertain about their compliance posture.

Key Areas of Change and Organizational Impact

1. Broader Definitions and Coverage

The new codes expand the definitions of ‘employee’, ‘worker’, and ‘wages’, potentially bringing in categories previously outside the scope of statutory coverage. For example, certain allowances and bonus structures that were excluded earlier may now be considered part of the wage base, triggering higher contributions and recalculated liabilities.

2. Centralized Registrations and Returns

Digitization of registrations, returns, and inspections intends to reduce administrative burden. However, inadequate readiness in digital systems, change management issues, and lack of clarity on procedural timelines can result in non-compliance or costly rectifications.

3. Enhanced Social Security Obligations

The Social Security Code expands coverage to gig and platform workers—requiring new

mechanisms for contribution tracking, benefit disbursement, and reporting. Organizations must build robust payroll and compliance systems to adapt effectively.

4. State-Specific Adaptations

While the codes provide a federal framework, states retain the right to issue rules and notifications for enforcement. Differential timelines and requirements across states increase complexity for multi-location employers.

5. Increased Enforcement Focus

Labour inspections are poised to be more structured—with defined checklists and digital reporting. Failure to comply could invite on-the-spot penalties and enhanced scrutiny from regulators.

Are Organizations Ready? A Preparedness Snapshot

Challenges

- Compliance Gaps: Many organizations still rely on fragmented legacy systems for statutory filings and wage computations.
- Documentation Deficiencies: Statutory records, policy documents, and audit trails are often inconsistent or incomplete.
- Limited Awareness: Middle management and HR teams may lack clarity on nuanced interpretation of the new provisions.
- Decentralized Practices: Multi-location entities with varied practices struggle to harmonize compliance frameworks.

Signs of Progress

- Companies with proactive internal audits and digital compliance tools have begun aligning processes ahead of enforcement waves.
- Industries with higher union presence and regulatory scrutiny (manufacturing, logistics, construction) are revisiting documentation frameworks and worker welfare protocols.

Despite these efforts, a majority of organizations still lack a systematic, risk-

based labour compliance program leaving them vulnerable to penalties, miscalculations, and reputational disruptions.

Labour Law Reforms Through a Risk Lens

Labour compliance is not merely a statutory checkbox it is a governance and risk control imperative. Non-compliance can lead to:

- Monetary penalties and back wages
- Disruption of operations during inspections
- Legal disputes and litigation
- Loss of investor confidence
- Adverse media and stakeholder scrutiny

Riskpro's Services: Enabling Preparedness & Compliance Excellence

At Riskpro, we recognize that labour law reforms present both a **challenge and an opportunity** for organizations to strengthen governance, mitigate operational risk, and build trust.

Here's how Riskpro partners with organizations through this transformation:

1. Labour Law Gap Assessment & Diagnostics

We conduct end-to-end compliance assessments mapped to the four labour codes and state-specific requirements. Our diagnostics identify:

- Statutory interpretation gaps
- Documentation deficiencies
- Payroll computation discrepancies
- Record-keeping risks

2. Policy & Process Harmonization

We assist organizations in revising HR and operational policies to align with updated definitions, wage structures, leave mandates, and welfare provisions. This includes:

- Wage structure reclassification
- Bonus & allowance integration
- Leave & attendance compliance
- Contract worker engagement protocols

3. Digital Compliance Enablement

Riskpro supports the implementation of digital frameworks for:

- Centralized registration and returns
- Statutory contribution tracking
- Automated alerts for filing deadlines
- Audit-ready record management

4. Training & Awareness Programs

We conduct targeted workshops for leadership, HR teams, and operational managers covering:

- Interpretation of labour codes
- Employer obligations and timelines
- Inspection preparedness
- Documentation best practices

5. Ongoing Compliance Monitoring & Advisory

Compliance is a continuous journey. Riskpro offers:

- Quarterly compliance reviews
- Regulatory update alerts (central and state)
- Quarterly governance dashboards for risk owners and leadership
- Support during inspections and dispute resolution

Conclusion

India's labour law reforms mark a landmark shift in how employers engage with statutory obligations, worker welfare, and governance expectations. While the codes aim to simplify compliance, true preparedness demands strategic planning, robust systems, and proactive risk management.

For organizations, the question is not just "Are we compliant?" but **"Are we ready to sustain compliance, govern responsibly, and build resilient human capital practices?"**

With a structured approach, governance-first mindset, and expert support, organizations can transform these reforms into an engine for sustainable growth, workforce trust, and regulatory confidence.



LABOUR LAW COMPLIANCE AUDIT – A PRACTICAL GUIDE

-ABIGAIL CRASTO

In today's regulatory environment, labour law compliance is no longer a back-office function managed solely by HR. It is a governance priority, a financial control mechanism, and a key contributor to ESG performance. With evolving frameworks such as the Code on Wages, 2019, Code on Social Security, 2020, Industrial Relations Code, 2020, and Occupational Safety, Health and Working Conditions Code, 2020, organizations must adopt a structured and audit-driven approach to ensure compliance.

A Labour Law Compliance Audit provides clarity, reduces risk exposure, and strengthens internal governance. This guide

outlines a practical roadmap for conducting an effective audit.

Why Conduct a Labour Law Compliance Audit?

A structured audit helps organizations:

- Identify statutory non-compliance risks
- Detect payroll miscalculations and contribution errors
- Assess contractor and third-party labour risks
- Prepare for government inspections
- Strengthen governance and ESG disclosures
- Avoid penalties, back wages, and reputational damage

An audit is not merely fault-finding it is a preventive risk management tool.

Step 1: Define the Scope of the Audit

The scope should be clearly documented and approved by management. It typically includes:

- Applicability analysis of central and state labour laws
- Employee classification (employee vs worker vs contractor)
- Wage structure review

- Statutory contributions (PF, ESI, gratuity, bonus, etc.)
- Registers and records maintenance
- Licenses and registrations
- Contractor compliance
- Workplace safety obligations

For multi-location entities, state-specific rules must also be mapped.

Step 2: Applicability & Registration Review

The audit begins by confirming:

- Whether the establishment is correctly registered under applicable labour statutes
- Validity and renewal status of licenses
- Display requirements (notices, abstracts, certificates)
- Contractor registrations and licenses

Many organizations face risk due to outdated registrations or non-renewal of licenses.

Step 3: Wage & Payroll Structure Examination

This is often the most critical component of the audit.

Key Checks:

- Whether wage components comply with definitions under the Code on Wages
- Minimum wage adherence as per state notifications
- Overtime calculations
- Bonus eligibility and computation
- Timeliness of wage payment
- Equal remuneration compliance

Incorrect wage structuring can lead to significant back-pay liabilities and statutory recalculations.

Step 4: Statutory Contributions & Returns

The auditor should verify:

- PF, ESI, and other contributions deposited within statutory timelines
- Correct contribution percentages

- Matching of payroll records with statutory filings
- Reconciliation of challans and employee registers
- Filing of periodic returns

Even minor errors in contribution base calculations can accumulate into large liabilities over time.

Step 5: Documentation & Record Verification

Maintaining proper documentation is crucial during inspections.

Audit should include review of:

- Employee appointment letters
- Attendance and leave records
- Muster rolls
- Wage registers
- Overtime registers
- Grievance redressal documentation
- Internal policies (POSH, leave policy, disciplinary policy, etc.)

Incomplete or inconsistent documentation often attracts penalties during inspections.

Step 6: Contractor & Third-Party Compliance Review

Organizations are increasingly held accountable for contractor compliance.

Audit should verify:

- Contractor agreements
- Proof of wage payments by contractors
- PF/ESI remittances for contract workers
- Valid labor licenses
- Indemnity and compliance clauses in contracts

Failure in contractor compliance can result in principal employer liability.

Step 7: Occupational Safety & Workplace Compliance

Under the Occupational Safety Code, safety

governance is a major focus.

Audit checks include:

- Safety committee formation
- Health and safety policy documentation
- Accident registers
- Insurance coverage
- Fire and emergency preparedness
- Statutory inspections and certifications

Workplace safety lapses carry both legal and reputational consequences.

Step 8: Reporting & Risk Categorization

An effective audit report should not merely list non-compliances. It should:

- Categorize findings (High / Medium / Low risk)
- Quantify potential financial exposure
- Provide corrective action timelines
- Assign accountability to specific functions
- Suggest control enhancements

A management summary should highlight strategic risks for leadership and board review.

Step 9: Remediation & Continuous Monitoring

Compliance is not a one-time exercise.

Best practices include:

- Quarterly internal compliance reviews
- Digital compliance tracking systems
- Regular training for HR and operations teams
- Periodic legal update monitoring
- Integration with enterprise risk management frameworks

Common Audit Findings

Across industries, some recurring issues include:

- Incorrect wage structuring
- Delayed statutory payments
- Missing contractor documentation
- Non-standardized appointment letters

- Inadequate state-specific compliance tracking
- Lack of board-level oversight

Recognizing these patterns allows organizations to proactively strengthen controls.

Labour Compliance Audit as a Governance Tool

Beyond statutory adherence, labour audits enhance:

- ESG reporting accuracy
- Investor confidence
- Operational stability
- Employee trust
- Brand reputation

Labour compliance today sits at the intersection of HR, finance, legal, and governance. A structured audit framework aligns all these functions under a unified compliance strategy.

Conclusion

A Labour Law Compliance Audit is not merely about avoiding penalties—it is about building resilience, strengthening governance, and protecting organizational reputation.

As India's labour law framework evolves under the four labour codes, organizations must move from reactive compliance to proactive audit-driven governance. A systematic, well-documented, and technology-enabled compliance program ensures that organizations are not only legally compliant but strategically prepared.

In a landscape of increasing regulatory scrutiny and stakeholder expectations, preparedness is not optional it is essential.

Top of Form



WHAT'S NEW AT RISKPRO

-ABIGAIL CRASTO

Advancing Labour Law Compliance, DPDPA Readiness & Smart Audit Innovation

As regulatory expectations intensify across India, 2026 has been a year of strategic expansion and sharper focus at Riskpro. With major shifts under India's new labour law regime and the enforcement momentum of the Digital Personal Data Protection Act, 2023, organizations are under increasing pressure to strengthen governance, documentation, and audit preparedness.

At Riskpro, we have responded with deeper domain expertise, integrated compliance solutions, and continued innovation through our DIY audit platform – Relixi.

Strengthened Focus on India's Labour Law Reforms

The consolidation of over 40 central laws into four codes has significantly altered the compliance landscape:

- Code on Wages, 2019
- Industrial Relations Code, 2020
- Occupational Safety, Health and Working Conditions Code, 2020
- Code on Social Security, 2020

These reforms impact wage structuring, social security contributions, contractor compliance, employee classification, and inspection processes.

What's New in Our Labour Practice:

- **Labour Code Readiness Assessments** across multi-state operations
- **Wage Structure Impact Analysis** under the revised wage definition
- **Principal Employer & Contractor Risk Reviews**
- **Inspection Preparedness & Mock Audit Programs**
- **ESG-Linked Labour Compliance Mapping**

We are increasingly seeing boards and leadership teams demand structured compliance dashboards and Riskpro has enhanced its reporting frameworks to provide risk visibility at the governance level.

Expanded DPDPA Implementation & Privacy Governance

With the operationalization of DPDPA, privacy compliance is no longer optional it is foundational. Organizations must now establish:

- Lawful processing frameworks
- Consent management systems
- Data subject rights mechanisms
- Breach reporting protocols
- Grievance redressal structures

Riskpro has expanded its privacy advisory to include:

- DPDPA Gap Assessments & Implementation Roadmaps
- Data Mapping & Processing Register Development
- Privacy Notice & Policy Drafting
- Employee Data Privacy Alignment
- Incident Response & Breach Simulation Exercises
- Quarterly Privacy Governance Reviews

For organizations operating globally, we continue to align our advisory services with frameworks such as the General Data Protection Regulation, ensuring consistency across jurisdictions.

Integrated Labour & Privacy Governance

A major shift this year has been our integrated approach recognizing that labour compliance and data protection are increasingly interconnected.

Employee data governance, payroll information security, background verification processes, and monitoring systems must now satisfy both labour law obligations and DPDPA requirements.

Riskpro's unified compliance framework ensures:

- Harmonized HR and privacy policies
- Secure payroll and statutory documentation practices
- Controlled access to employee records
- Defined data retention schedules
- Reduced cross-functional compliance silos

Continued Innovation: Relixi – Our DIY Audit Tool

A key highlight this year is the continued enhancement of Relixi, Riskpro's proprietary DIY audit platform.

Relixi was designed with a clear objective: to democratize compliance readiness and make audits proactive rather than reactive.

What Relixi Offers:

- Self-assessment modules for labour law compliance
- DPDPA readiness checklists
- Automated compliance scoring
- Risk-based gap identification
- Actionable remediation guidance
- Downloadable audit-ready reports

Relixi enables organizations especially growing enterprises and multi-location businesses to:

- Monitor compliance health in real time
- Identify gaps before inspections
- Prepare internally before formal audits
- Track remediation progress
- Maintain audit trails systematically

With new modules now aligned to India's labour codes and DPDPA obligations, Relixi has evolved into a practical compliance companion for leadership and HR teams.

Technology-Enabled Governance

Beyond Relixi, Riskpro has strengthened its compliance technology integration capabilities:

Digital statutory calendars

-
- Automated filing alerts
 - Privacy compliance trackers
 - Governance dashboards for leadership reporting
 - Centralized documentation repositories

This shift toward automation reduces manual dependency and enhances defensibility during regulatory scrutiny.

Capability Expansion & Client-Centric Enhancements

To support these developments, Riskpro has:

- Expanded its specialist teams in labour compliance, privacy audits, and ESG governance
- Introduced advanced compliance health scoring models
- Launched sector-specific compliance frameworks
- Enhanced client portals for audit documentation access
- Rolled out structured quarterly governance review sessions

Looking Ahead

Regulatory enforcement is becoming more data-driven, digital, and accountability-focused. Labour inspections are expected to intensify. Privacy breaches are under greater scrutiny. ESG disclosures are becoming more structured.

At Riskpro, our path forward is clear:

- Deep expertise in labour and privacy governance
- Technology-led compliance monitoring
- Proactive audit readiness through Relixi
- Integrated risk advisory across domains

Conclusion

2026 is not just about adapting to regulatory change it is about building sustainable governance frameworks that endure.

With strengthened focus on labour law reforms, structured DPDPA implementation,

and continued innovation through Relixi, Riskpro is enabling organizations to move beyond compliance anxiety toward compliance confidence.

The future of governance is proactive, digital, and integrated—and Riskpro is proud to be at the forefront of that transformation.



RELIXI: THE DIY COMPLIANCE PLATFORM MAKING ENTERPRISE-GRADE SECURITY ACCESSIBLE

-EKTA GADA

In an era where regulatory frameworks like ISO 27001, SOC 2, DPDPA, and PCI DSS demand ever more rigorous compliance, organizations have traditionally faced a painful choice: hire expensive consultants, buy bloated enterprise GRC suites, or cobble together spreadsheets and hope for the best. Relixi, built by Riskpro India, offers a compelling third path a first-of-its-kind DIY compliance management platform that combines deep, real-world content with powerful automation.

What Is Relixi?

Relixi is a B2B SaaS compliance automation platform focused on the Security and Privacy domains. Its core promise is enabling organizations to perform automated, paperless compliance assessments without needing a dedicated in-house compliance team or an external auditor's retainer. The platform covers ISO 27001, SOC 2, DPDPA (India's Digital Personal Data Protection Act), PCI DSS, internal audits, risk management, and more all within a single, unified interface.

The DIY Differentiator

The platform is designed for organizations that want to own their compliance journey rather than outsource it.

Relixi achieves this through:

Deep, pre-built content. Rather than offering empty frameworks that require users to interpret controls and build policies from scratch, Relixi comes loaded with real-world content control mappings, policy templates, evidence requirements, and best practices all aligned to specific regulatory standards. This dramatically reduces the learning curve.

Guided workflows. The platform doesn't just present a checklist; it walks users through each step of the compliance process, from gap assessment through remediation to audit readiness. This structure is particularly valuable for organizations pursuing compliance for the first time.



Modular architecture. Relixi is built on a modular framework where each compliance domain ISO 27001, SOC 2, Vendor Risk Management, and so on can be enabled as a separate module. Organizations can start small and expand coverage as their needs grow.

Automation and paperless operations. Manual evidence collection, control testing, and reporting are replaced with automated workflows that track compliance status in real time, flag gaps, and generate audit-ready reports.

Who Needs Relixi?

The platform is particularly well-suited for:

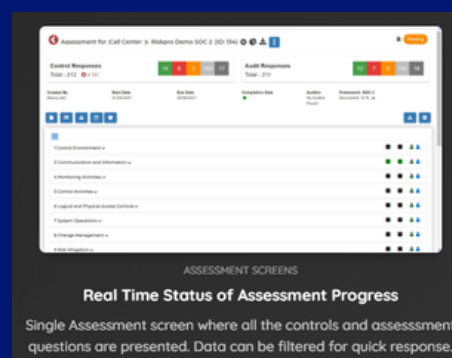
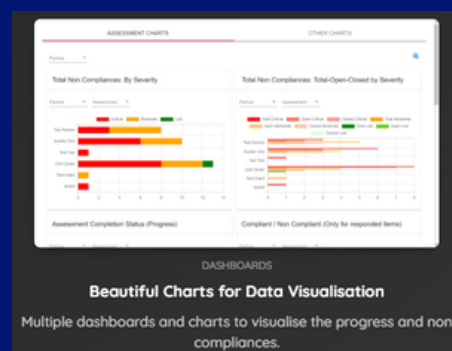
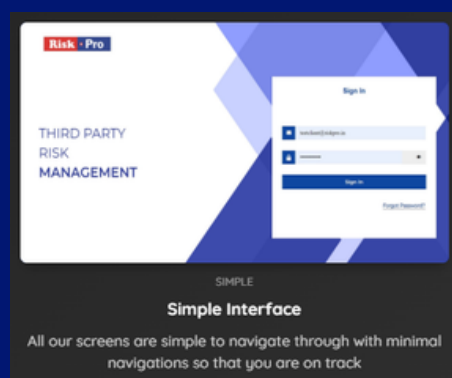
- Mid-market companies that have outgrown spreadsheet-based compliance but aren't ready for the cost and complexity of enterprise GRC systems.
- Startups seeking SOC 2 or ISO 27001 certification for the first time, where guided DIY tools can significantly reduce both time-to-certification and external consulting costs.
- Indian organizations navigating DPDPA compliance, given Relixi's native support for India's data protection regulations.
- Organizations managing multiple frameworks simultaneously, where the modular approach allows consolidated oversight without redundant effort.

Getting Started

Relixi is accessible through its web application at app.relixi.com, with Riskpro offering a free 30-day trial with no obligations and account creation within one business day. This low-friction onboarding reflects the platform's DIY ethos organizations can evaluate its fit for their needs without sales calls or lengthy procurement cycles.

The Bottom Line

Compliance is no longer optional for most organizations, but it doesn't have to be a black hole of consulting fees and administrative overhead. Relixi occupies a valuable niche: a platform that treats compliance as a capability that organizations can build themselves, not just a service they buy. For teams that want to move fast, stay audit-ready, and develop lasting compliance expertise in-house, it's worth a serious look.



OUR WORK

Inside View of our Application

The screenshot displays the 'ROPA' (Records of Processing Activities) interface. At the top, the title 'ROPA' is followed by the subtitle 'Records of Processing Activities'. Below this, a section titled 'Processing Activity' is shown with a dropdown arrow. The form contains several fields: 'Processing Activity Name' with a red asterisk and a placeholder 'Add Response'; 'Purpose of Processing' with a subtitle 'Add summary of processing, use this only for major processing.' and a placeholder 'Eg Storage, sending emails'; and 'Categories of Processing' which lists various data types with checkboxes. The categories include: Govt ID, Demographic, Health Data, Passport, Bank Account Details, Address, Date of Birth, E-mail ID, Mobile Number, Designation, Employer/Company Name, Educational Qualifications, Employment Details, Cookies, Google AdWords, Google Play, Geolocation, Salary Information, City, Name, Gender, Religion, Credit Card, and others. The interface is clean and modern, with a blue header and white form fields.

RISK MANAGEMENT

Fully Configurable Forms

Centrally manage all forms and content to truly make this platform with unlimited modules.



PARTNERSHIP PROGRAM AT RISKPRO

-ABIGAIL CRASTO

Building Strategic Alliances for Scalable Risk & Compliance Solutions

In today's interconnected business ecosystem, no organization operates in isolation. Clients increasingly seek integrated, multi-disciplinary solutions that combine domain expertise, technology enablement, regulatory insight, and operational scalability. Recognizing this shift, Riskpro has developed a structured Partnership Program designed to create collaborative value for clients, partners, and the broader compliance ecosystem.

The Riskpro Partnership Program is built on a simple philosophy: strong alliances create stronger governance outcomes.

Why Partnerships Matter in the Risk & Compliance Landscape

Risk management today spans multiple domains:

- Information Security & Cybersecurity
- Data Privacy & Regulatory Compliance
- Labour Law & ESG Governance
- IT Advisory & Controls
- GRC Automation & Technology Enablement
- Audit & Assurance Services

No single organization can be a specialist in every niche area at scale. Clients expect seamless service delivery across geographies and regulatory frameworks such as the Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation, alongside evolving labour law codes and cybersecurity mandates.

Through structured partnerships, Riskpro enables:

- Broader service reach
- Deeper domain specialization
- Faster go-to-market capabilities
- Stronger cross-border compliance support

-
- Integrated advisory and technology delivery

Objectives of the Riskpro Partnership Program

The program is designed to:

1. Expand service capabilities through complementary expertise
2. Strengthen market access across geographies and sectors
3. Deliver technology-enabled compliance solutions
4. Enhance value for shared client ecosystems
5. Drive sustainable revenue growth for partners

We view partnerships as long-term strategic alliances not transactional referral arrangements.

Types of Partnerships

Riskpro collaborates across multiple partnership categories:

1. Technology Partners

Providers of GRC platforms, privacy automation tools, cybersecurity solutions, and compliance monitoring software.

We support implementation, readiness assessments, risk mapping, and audit validation ensuring clients derive measurable value from technology investments.

2. Channel & Referral Partners

Consulting firms, CA firms, legal advisors, HR advisory firms, and IT service providers who seek to extend their service portfolio in:

- SOC 1 & SOC 2 readiness
- ISO 27001 implementation
- Privacy audits
- Labour compliance audits
- ESG-linked governance advisory

3. International Advisory Partners

Cross-border collaborations enable support for global regulatory frameworks and multinational compliance requirements.

4. Strategic Business Alliances

Organizations seeking co-branded offerings, joint webinars, thought leadership initiatives, and industry roundtables.

What Makes the Riskpro Partnership Model Unique?

Structured Onboarding

Every partner undergoes a structured onboarding process covering service alignment, market positioning, pricing framework, and delivery standards.

Clear Commercial Framework

Transparent revenue-sharing models and clearly defined engagement structures ensure predictability and mutual growth.

Delivery & Technical Support

Riskpro provides technical advisory, audit frameworks, policy templates, compliance checklists, and expert support during project execution.

Sales & Pre-Sales Enablement

We support partners with:

- Proposal templates
- Pitch decks
- Compliance readiness checklists
- Pre-sales technical discussions
- Joint client meetings

Thought Leadership Collaboration

Partners gain access to joint branding opportunities, webinars, industry publications, and participation in Riskpro's annual magazine and compliance forums.

Value Delivered to Clients

Through the Partnership Program, clients benefit from:

- End-to-end compliance coverage
- Integrated technology and advisory solutions
- Faster project execution
- Consistent governance standards
- Scalable support across locations

This integrated model reduces fragmentation and ensures clients receive cohesive, strategic guidance rather than siloed services.

Governance & Quality Assurance

Riskpro maintains strong internal quality controls across all partnership engagements. This includes:

- Standardized audit methodologies
- Review checkpoints
- Risk-based documentation frameworks
- Defined escalation protocols
- Client feedback loops

Partnership success is measured not only by revenue but by client satisfaction and compliance outcomes.

Future Vision

As regulatory landscapes evolve across privacy, cybersecurity, labour compliance, and ESG collaboration will become even more critical. Riskpro aims to expand its partnership ecosystem across India, the Middle East, Europe, and emerging digital markets.

Our focus is on:

- AI governance advisory partnerships
- ESG compliance alliances
- Privacy automation collaborations
- Cybersecurity technology integrations

The future of compliance is integrated, technology-enabled, and partnership-driven.

Conclusion

The Riskpro Partnership Program reflects our belief that growth is stronger when shared. By combining expertise, expanding capabilities, and aligning strategic objectives, we create a collaborative ecosystem that delivers measurable governance impact.

For organizations seeking to strengthen their service offerings, enter new markets, or enhance compliance delivery capabilities, Riskpro's Partnership Program offers a

structured, scalable, and mutually rewarding model.

Together, we don't just manage risk we build resilient enterprises.



RISKPRO ACADEMY: INDIA'S PIONEERING PLATFORM FOR RISK, COMPLIANCE, AND GOVERNANCE EDUCATION

-EKTA GADA

In an era where regulatory landscapes shift rapidly and financial crimes grow increasingly sophisticated, the demand for skilled risk and compliance professionals has never been higher. Enter Riskpro Academy (academy.riskpro.in) the e-learning and certification division of Riskpro India Ventures Private Limited, a specialized risk management consulting firm founded in 2008.

With over 17 years of deep domain expertise, Riskpro Academy has established itself as India's pioneering online learning platform dedicated exclusively to governance, risk, and compliance (GRC) education. The academy currently offers 75+ specialized courses spanning risk management, compliance, financial crimes, forensic accounting, and investigation domains – making it one of the most comprehensive GRC learning ecosystems in the country.

Our Mission

Riskpro Academy's mission is clear: to democratize risk and compliance education by delivering practitioner-driven, industry-recognized training that bridges the gap between academic theory and real-world application.

The academy is committed to empowering professionals at every career stage, from fresh graduates seeking entry into the compliance field to seasoned executives navigating complex regulatory environments. Every course is designed to equip learners with practical knowledge they can apply immediately in their roles, helping organizations build stronger defence mechanisms against financial crime and regulatory failure.



Course Portfolio

Riskpro Academy's curriculum is organized across **seven core domains**, each addressing a critical pillar of the modern risk and compliance landscape:

1. Risk Management – Courses include Enterprise Risk Management (ERM), Operational Risk Management, Basel & Financial Risk, and Credit & Liquidity Risk Management. These programs equip professionals with frameworks to identify, assess, and mitigate organizational risks systematically.

2. Compliance & Global Regulations – The academy offers the flagship Certified Global Compliance Specialist (GCS) program, along with specialized courses on FCPA & Anti-Corruption, Internal Financial Controls (IFC/ICFR), and SEBI LODR compliance.

3. Anti-Money Laundering – A comprehensive suite covering AML Certification, KYC Compliance, and Transaction Monitoring essential knowledge in an age where money laundering threats are more complex than ever.

4. Fraud & Forensic Accounting – Courses include Forensic Accounting & Fraud Examination, Fraud Risk Management, Fraud Investigation & Internal Audit, and the Certified Fraud Analytics Specialist program.

5. Audit – Programs such as Risk-Based Internal Audit (RBIA) and Internal Audit Fundamentals help professionals build robust audit capabilities aligned with global standards.

6. Cyber & Information Security – Courses on Cybersecurity Compliance and Cyber Threat Intelligence address the growing intersection of technology risk and regulatory requirements.

7. Emerging Domains – Forward-looking courses include the Certified ESG Expert program, Blockchain for the Financial Industry, and the Certified Tax Fraud Analyst (CTFA), reflecting the academy's commitment to staying ahead of industry trends.

Flagship Programs

Certified Global Compliance Specialist (GCS) – This certification provides a comprehensive overview of critical compliance topics, including Prevention of Insider Trading, Anti-Money Laundering, FCPA, Global Compliance frameworks, SEBI LODR requirements, building effective compliance frameworks, Anti-Bribery and Anti-Corruption, HIPAA, and GDPR. Course fee is just ₹1,000 remarkably affordable for the breadth of content covered. [Enroll here.](#)

Anti-Money Laundering (AML) Certification (Exam Only) – In-depth coverage of AML regulations, KYC norms, transaction monitoring, and suspicious activity reporting essential knowledge for compliance officers and financial crime investigators. [View course.](#)

Enterprise Risk Management (ERM) Certification (Exam Only) – A comprehensive examination-based certification for professionals looking to validate their expertise in enterprise-wide risk management frameworks. [View course.](#)

Why Choose Riskpro Academy?

Flexibility – The platform offers the freedom to learn anytime, anywhere, accommodating diverse schedules and allowing learners to pace their education according to their own convenience.

Global Reach – Courses are available in multiple languages, ensuring accessibility for a diverse global audience.



Accessibility – As a fully online platform dedicated to risk, compliance, and privacy education, learners gain access to a wealth of information and resources regardless of their geographical location, opening doors to a global learning community.

Self-paced Learning – Participants can complete courses at their own pace with no defined timelines for completion, making it ideal for working professionals balancing career and continuing education.

Cost-Effectiveness – Compared to traditional classroom learning, most courses are

How to Register on Risk Academy?

- Participants who would like to view or enroll for any of our risk and compliance courses simply need to visit - <https://academy.riskpro.in/>

Corporate Training - Customized

We also provide customized corporate training for minimum batch size of 10 employees. To know more, please email info@riskpro.in



RISKPRO IN 2025: STRENGTHENING GOVERNANCE, ENABLING TRUST

-RUCHITA SOBALKAR

At Riskpro, governance and trust are not limited to business processes and client engagements they are deeply embedded in our people practices and organizational culture. As we move into 2025, the Human Resources function continues to play a critical role in strengthening governance, building transparency, and creating a workplace founded on trust, accountability, and growth.

In today's dynamic work environment, organizations are expected to maintain not only operational excellence but also ethical and employee-centric practices. At Riskpro, HR acts as a strategic partner in aligning people practices with organizational values

and long-term business goals. From recruitment and onboarding to employee engagement, performance management, and policy implementation, governance remains at the core of every HR initiative.

Over the past year, we have focused on building structured HR processes that promote fairness, consistency, and employee well-being. Clear communication, transparent policies, timely feedback, and compliance-driven practices have helped us strengthen employee confidence and organizational discipline. Initiatives related to performance management, learning and development, employee benefits, and workplace ethics continue to evolve in line with organizational growth.

One of the key priorities for HR in 2025 is creating a culture of trust and collaboration. Employees perform best when they feel heard, valued, and supported. Through regular employee interactions, leadership connect sessions, engagement activities, and open communication channels, we aim to foster a positive and inclusive work environment.

As organizations grow, maintaining strong governance also requires continuous focus on compliance, documentation, process standardization, and accountability. HR has been actively working toward strengthening these areas while ensuring that employees experience a smooth and supportive work culture.

At Riskpro, we strongly believe that people are our greatest strength. Enabling trust begins internally through ethical leadership, transparent communication, employee empowerment, and a culture of respect. As we continue our journey in 2025, HR remains committed to supporting both organizational growth and employee success while building a resilient and future-ready workplace.





BUILDING EXPERTISE AT RISKPRO

-RUCHITA SOBALKAR

At Riskpro, building expertise is not viewed as a one-time effort but as a continuous journey of learning, development, and growth. In an industry where technologies, regulations, and client expectations are constantly evolving, developing skilled and future-ready professionals has become one of the organization's key priorities. Human Resources plays an important role in creating opportunities that help employees strengthen both technical and professional capabilities.

Riskpro believes that every employee has the potential to grow when provided with the right environment, guidance, and exposure. From onboarding programs to ongoing learning initiatives, the organization focuses on creating a culture that encourages continuous improvement and knowledge sharing.

Employees across various domains such as

Information Security, ISO, PCI-DSS, SOC operations, IT Audits, GRC, Compliance, and Cybersecurity are regularly exposed to diverse projects and client environments. This practical exposure helps individuals enhance their technical understanding, improve problem-solving skills, and gain confidence in handling responsibilities independently.

HR, along with business leaders, continuously works toward identifying skill gaps and encouraging learning through certifications, internal training sessions, mentorship programs, and cross-functional collaboration. Senior team members actively support and guide employees, helping them navigate challenges and build expertise through practical learning experiences.

Apart from technical development, equal importance is given to communication skills, leadership qualities, teamwork, and professional behavior. Building expertise today requires a balance of technical competence and interpersonal effectiveness. Through continuous feedback and employee development initiatives, Riskpro aims to nurture well-rounded professionals who can

contribute effectively to both clients and teams.

Another important aspect of expertise-building at Riskpro is creating a supportive learning culture. Employees are encouraged to ask questions, share knowledge, take ownership, and step out of their comfort zones. This collaborative environment helps individuals grow with confidence while strengthening overall organizational capability.

As Riskpro continues to expand, investing in employee development remains a strategic priority. By empowering employees with learning opportunities, mentorship, and career growth, the organization is building a strong foundation for future success while creating professionals who can lead with knowledge, integrity, and confidence.



RISKPRO'S 2025 SOCIAL CALENDAR: BUILDING CONNECTIONS, SHARING KNOWLEDGE, CELEBRATING SUCCESS

-ABIGAIL CRASTO

At Riskpro, 2025 was more than a year of delivering risk, compliance, cybersecurity, and privacy solutions it was a year of building stronger connections with our clients, partners, and employees. Through industry events, knowledge-sharing initiatives, and team celebrations, we continued to strengthen our culture of collaboration, learning, and innovation.

Engaging with the Industry

Throughout the year, Riskpro actively participated in several key industry events, providing opportunities to engage with professionals, exchange insights, and contribute to important conversations around governance, risk, compliance, privacy, and cybersecurity.

Our team attended the ISACA event, connecting with information security, audit, and governance professionals from across the industry. The event provided valuable perspectives on emerging risks, cybersecurity trends, and the evolving regulatory landscape.

We also participated in the Cyber Security Expo in Mumbai, where our team interacted with technology leaders, security practitioners, partners, and organizations seeking innovative approaches to cyber risk management. The event enabled us to showcase our expertise while gaining deeper insights into the challenges organizations face in an increasingly digital world.



In Pune & Mumbai, Riskpro hosted and participated in a dedicated Data Protection and Digital Personal Data Protection Act (DPDPA) event. The session brought together privacy professionals, business leaders, and compliance practitioners to discuss practical approaches to implementing India's evolving privacy framework and preparing organizations for compliance.

Driving Knowledge Through Webinars

Knowledge sharing remained a cornerstone of our engagement strategy in 2025. Through our monthly webinar series, we brought together experts, clients, and industry professionals to discuss some of the most pressing topics in governance, risk, and compliance.

Key themes covered during the year included:

- Digital Personal Data Protection Act (DPDPA) compliance and implementation
- Labour Law reforms and workforce compliance
- Virtual Chief Information Security Officer (vCISO) services and cybersecurity leadership
- Emerging risk and governance trends
- Best practices for building resilient compliance programs

These sessions enabled participants to gain practical insights while fostering meaningful discussions around today's evolving regulatory and risk environment.

Bringing Teams Together

While professional growth and client engagement remain important, we also believe that strong organizations are built on strong relationships.

The year began with our annual company picnic in January, bringing together team members from different locations and functions. The event provided an opportunity for colleagues to connect beyond their day-to-day responsibilities, strengthen relationships, and celebrate the collaborative culture that defines Riskpro.

As a people-focused organization, we also celebrated important cultural festivals together. Our Ganpati celebrations filled the office with enthusiasm, unity, and tradition, while our Diwali celebrations brought colleagues together to share festive moments, recognize achievements, and celebrate another successful year.

These occasions remind us that while our work is focused on helping organizations manage risk and build trust, our greatest strength remains our people.

Looking Ahead

As we reflect on 2025, we are proud of the relationships we have built, the knowledge we have shared, and the culture we continue to nurture. Whether through industry events, educational initiatives, or team celebrations, every activity contributed to our mission of enabling trust, fostering expertise, and creating lasting impact.

As we move into the year ahead, Riskpro remains committed to staying connected with our community, empowering organizations through knowledge, and creating opportunities for our people to grow, collaborate, and succeed together.

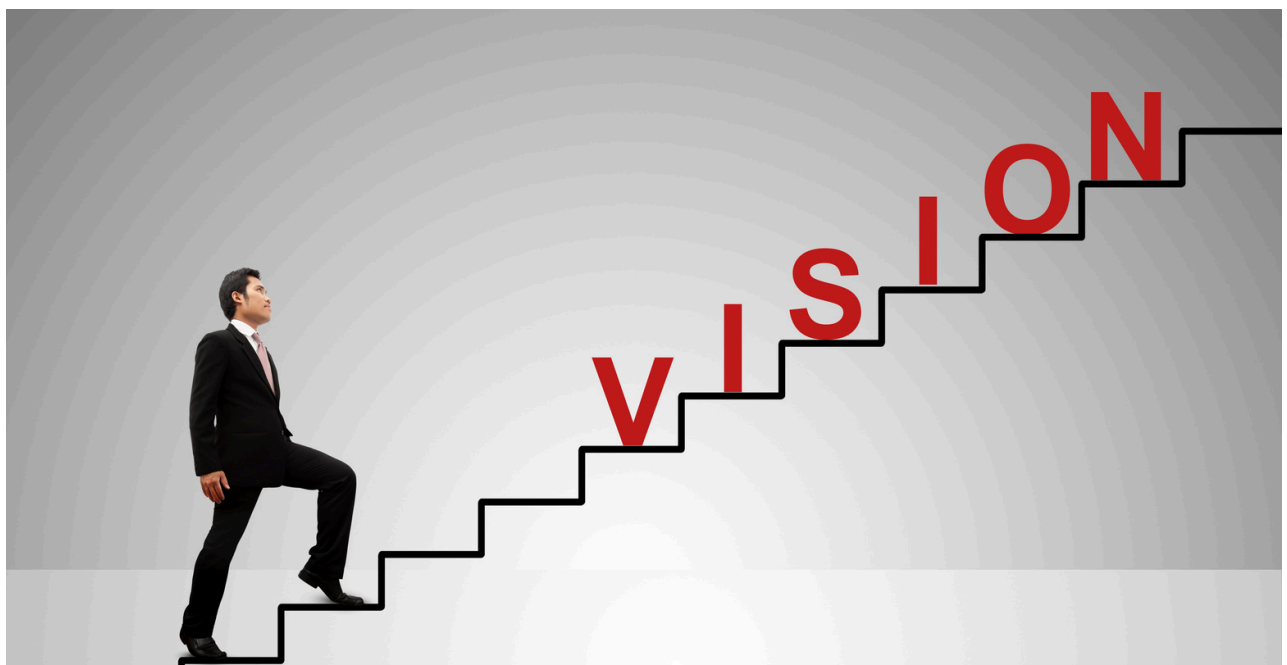
OUR VISION FOR THE YEAR AHEAD

-NITESH SHANBAGH

Riskpro India Ventures Pvt. Ltd., over the last decade plus, has been building trusted environments for our customers. As a single-point partner, we have continuously provided risk and compliance solutions across a broad-spectrum covering Enterprise Risk, Legal Compliance, Information Security and Privacy. Recently, a rapid growth in the global digital footprint, automation and AI driven the need and demand for assurance and compliance services in security and privacy. We have shifted our focus to this customer demand.

Riskpro's assurance and audit services enable customers to chart their digital compliance journey to demonstrate their security posture to their customers and stakeholders by complying to standards such as SOC2, ISO 27001, PCI DSS, HIPAA, GDPR, CCPA and DPDPA among others. Riskpro also provides pen testing and vulnerability assessment and other cybersecurity solutions. Riskpro also through partners provides technology solutions for cybersecurity, data discovery and protection and compliance automation.

Riskpro has gradually established itself, with over 1,000 clients, among a variety of startups, MSME's and fintec companies as a provider of assurance, audit and consulting services. Riskpro has been making a conscious effort to move up the value chain to provide solutions which enable companies become digitally robust and compliant. Riskpro's vision is to be a partner in the digital rollout, expansion and compliance journey. Riskpro intends to provide solutions and services for planning and building its customers' digital framework and monitoring their compliances and keeping them



audit ready. These solutions cover strategy, decisioning on automation and tooling, implementation, and providing fragmented, flexible and financially sustainable resourcing solutions to its customers.

Riskpro's team consists of nearly 100 full-time professionals, over 200 on-call specialists and 50+ active partners. We have developed significant expertise and experience in the digital, cybersecurity infosec and privacy domains and having audited and guided several firms (1500 SOC2 audits). The skill set of Riskpro's experienced staff makes Riskpro well equipped to cater to a broader set of customers' needs, providing increasing value to our customers. Deepening the our engagement and relationship.

Through, 2026 and beyond Riskpro will continue to offer solutions in technology, consulting and implementation in digital space and cybersecurity to our customers, audit readiness, and flexible and virtual resourcing solutions to its customers, keeping in min global political, economic and business uncertainties. We should see a significant shift in the revenue profile of Riskpro from audits to consulting, technology, products and resourcing as we leverage ...

- i) our large customer base to provide a broader and deeper set of value added services,
- ii) our significant experience and skill-sets the Riskpro team has built across cybersecurity, privacy and digital domains
- iii) our strong partner network that we have built over the years and maintain to this day.

We look forward to Building a trusted environment for your business.



Contact Details



Email Address

For any queries reach out
to us at info@riskpro.in



Website

www.riskpro.in

For regular updates follow us at



YouTube

Are you ready to Enhance your Risk and Compliance Knowledge?

Look no further than the
[Riskpro Academy](#) & Library
– your ultimate destination
for expanding your horizons,
honing your skills, and
enriching your mind.





Risk • Pro

Building a trusted environment

**THANK
YOU**

Designed By:
Ekta Gada

Editor:
Abigail Crasto