



**Risk • Pro**

Building a trusted environment

# 2025 **RISKPRO** **MAGZINE**

CELEBRATING  
GROWTH AND  
PROGRESS 2024-25

---

# Table of Contents:

1. Founders Note
2. About Riskpro
  - Riskpro Overview
  - Riskpro Mission Statement
  - Riskpro Services
3. Industry Insights and Trends
  - Emerging Risks: AI, Blockchain Vulnerabilities, Climate Risks
  - SOC Framework Updates: Strengthening Security in an Evolving Landscape
4. Strategies and Tools
  - Artificial Intelligence & Machine Learning
  - Mandatory Penetration Testing: A Critical Requirement for Cyber Resilience
  - The Importance of AI Auditing: Ensuring Transparency and Compliance
  - Strengthening Financial Systems Against Illicit Activities: The Imperative of Anti-Money Laundering (AML)



---

# Table of Contents:

## 5.Regulatory Updates

- Global Risk Management Landscape: Key Regulatory Developments
- Compliance best practices and upcoming changes to watch for

## 6.Risk Management Around the World

- Global Risk Management: A Comparative Analysis of Risk Landscapes Across Regions
- Collaboration Efforts in International Risk Management

## 7.Sustainability & GRC Integration

- Holistic Risk Management: Integrating Governance, Risk, and Compliance for Enhanced Decision-Making
- What does a Sustainability Partner look like?

## 8.Company Highlights

- Riskpro's Growth in 2024
- Partnership at Riskpro.
- Highlights from 2024 Conferences, Webinars, and Workshops.
- Training and Learning – Riskpro Academy
- Riskpro HR Initiatives

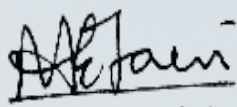
## 9.Our Team

## 10.Contact Us





# Founders Note



**MANOJ JAIN**  
CEO, RISKPRO INDIA



Dear Readers,

2024 was a transformative year for Riskpro—marked by growth, innovation, and a strengthened commitment to risk management. As risks evolved across cybersecurity, regulations, and global markets, we guided businesses through uncertainty with resilience and clarity.

We deepened our focus on GRC automation, cybersecurity, and data privacy, helping clients adopt smarter, tech-enabled solutions. Our enhanced SOC 1 & SOC 2 readiness services and global policy gap assessments have supported organizations in aligning with ever-changing compliance landscapes.

Risk today demands strategic foresight. At Riskpro, we remain dedicated to empowering businesses with the tools and insights to turn risk into opportunity.

Thank you to our clients, partners, and team for your trust and support. Here's to another year of impact and innovation.



# About Our Company


## Who We Are And What We Do!

Riskpro India Ventures Private Limited ("Riskpro India") is a specialized Risk Management and compliance consulting company in India. We are one of the fastest-growing risk consulting firms in India managed by experienced professionals with experiences across various industries. With over 12+ years of industry experience, over 1000+ clients and having 90+ team members our firm has achieved significant milestones and growth. We have established over 15+ strategic alliance enhancing our capabilities and reach to over 500 cities.

---

# Mission

Building a trusted environment by  
helping businesses comply and  
manage risks



## OUR Services

---

Our solutions extend beyond traditional  
risk management offerings and are  
categorized into the following 5  
verticals:

- Risk Advisory
  - IT Advisory
  - GRC Technology
  - GRC Trainings
  - Risk Resources
- 







## Risk Advisory

- Risk Based Internal Audit
- Internal Financial Controls ( IFC)
- Vendor Risk Management (TPRM)
- Regulatory Compliance Consulting
- SOX Compliance
- Environment Social Governance (ESG)
- Standard Operation Procedures (SOPs)
- Enterprise Risk Management
- Operational Risk Management
- Branch Audits
- Fraud and Forensics
- Social Media Risk Management



## IT Advisory

- SOC (SSAE) Audits
- Digital Personal Data Protection Act 2023 (DPDPA)
- CMMC
- Microsoft SSPA
- Data Analytics
- GDPR
- ISO 27001
- 21 CFR Part 11
- HIPAA Compliance
- VAPT
- PCI DSS
- Cyber Security Advisory
- Business Continuity/Disaster Recovery
- NIST Compliance
- IT General Controls (ITGC)



## Technology

- Internal Audit Software
- Third Party Risk Software (TPRM)
- Legal Compliance Software
- Labour Compliance Automation Software
- Secretarial Compliance Automation Software
- Treasury Management Software (TMS)
- Risk Management Software
- Contract Management Software
- Whistleblowing Software
- Cyber Security Software
- GRC Software
- Data Privacy Software
- Document Management Software



## Trainings

- Risk Training/ ERM
- Fraud Risk Training
- Anti Bribery / Corruption Training
- Board Training
- Operational/ Credit Risk Training
- POSH Training
- Risk Based Internal Audit Training
- Vendor Risk Management Training
- Regulatory Compliance Training
- ISO 31000 Training
- AML Training
- Information Security Awareness Training
- Privacy Awareness Training
- Cyber Security Training
- ITGC Training





## Recruitment

- Virtual CISO
- Virtual Risk Manager
- IT Audit Professionals
- Internal Audit Professionals

*Our*



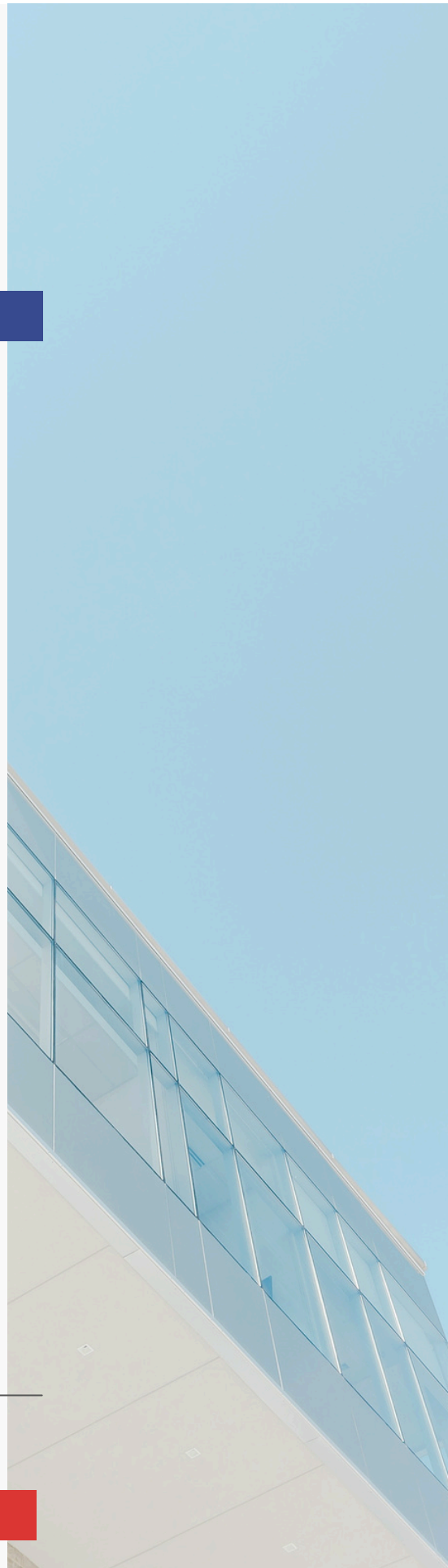
*Verticals*

---



# Industry Insights and Trends

---





---

# Emerging Risks Due to AI, Blockchain, and Climate Change in India

-Ashok Agarwal



As developing nations like India embrace transformative technologies such as Artificial Intelligence (AI) and Blockchain, they face a unique set of emerging risks. These risks, coupled with climate change challenges, pose significant threats to economic stability, regulatory frameworks, and social structures.

## **1. AI-Related Risks**

- **Bias & Discrimination:** AI models trained on biased datasets can perpetuate social inequalities in context of India, affecting hiring, lending, and law enforcement decisions.
- **Job Displacement:** Automation in sectors like Banking, Non-Banking, FinTeh, manufacturing, customer service, and logistics could lead to unemployment, especially for low-skilled workers.
- **Privacy & Data Security:** AI-driven surveillance, facial recognition, and data processing increase risks of data misuse, unauthorized tracking, and cyber threats, in context of DPPDP Act Vs. Challenges encountered in implementation by Industry leaders.
- **Regulatory & Ethical Concerns:** The absence of strong AI / IT Governance frameworks can lead to ethical dilemmas, such as deepfakes, misinformation,

---

and AI-generated fraud.

## **2. Blockchain-Related Risks**

- **Regulatory Uncertainty:** The legal status of cryptocurrencies and smart contracts remains unclear in India and adequate regulatory guidelines, leading to potential financial instability.
- **Fraud & Scams:** Unregulated blockchain projects and Ponzi schemes continue to deceive investors, causing financial losses.
- **Security Vulnerabilities:** Smart contract bugs and blockchain network hacks can lead to irreversible financial losses.
- **Energy Consumption:** Blockchain mining, especially Proof-of-Work models, contributes to significant energy usage, exacerbating environmental concerns.

## **3. Climate Change Risks**

- **Extreme Weather Events:** Rising temperatures, floods, and droughts threaten agriculture, infrastructure, and urban sustainability.
- **Water & Food Scarcity:** Climate variability impacts crop yields, leading to food insecurity and inflation.
- **Health Risks:** Increased heatwaves, air pollution, and vector-borne diseases disproportionately affect vulnerable populations.
- **Economic Disruptions:** Climate-related disasters can strain government resources, disrupt supply chains, and increase insurance costs.
- **Political ethics Vs Nation Security :** Weak opposition without national interest may create a confusion among Indian Talents – Country may face threats of drain may if not adequately handled by Government of India. Vote politics Vs Freebees distribution may lead India in economic crisis.

## **Conclusion**

Government of India must proactively address these emerging risks by implementing robust regulatory frameworks, promoting ethical AI and Blockchain adoption, and enhancing climate resilience strategies. Collaboration between policymakers, businesses, and academia is essential to mitigate these risks and ensure sustainable growth in the digital era.



---

# SOC Framework Updates: Strengthening Security in an Evolving Landscape

-Ekta Gada



As organizations continue to navigate an increasingly complex digital landscape, the need for robust security frameworks has never been more critical. The updates anticipated for the Service Organization Control (SOC) 2 and SOC 3 frameworks reflect an evolving emphasis on risk management, third-party security, and cloud privacy. These changes are designed to address the growing array of threats and enhance operational transparency, ensuring organizations can effectively protect sensitive data and maintain trust with stakeholders.

## **Understanding SOC 2 and SOC 3 Frameworks**

SOC 2 is particularly pertinent for technology and cloud computing organizations handling customer data. It focuses on five "trust service criteria": security, availability, processing integrity, confidentiality, and privacy. The framework ensures that service providers manage data in a way that protects the interests of the organization and the privacy of its clients.

SOC 3, while similar to SOC 2, is designed for a broader audience. It provides a general report that outlines the same trust service criteria but is less detailed,

---

making it suitable for marketing purposes and demonstrating compliance to clients and stakeholders without revealing sensitive information.

### **Anticipated Updates: Focus Areas**

- **Enhanced Risk Management**

Upcoming SOC updates will prioritize comprehensive risk management, promoting a proactive culture of identifying and mitigating risks.

- **Third-Party Security**

With increased reliance on vendors, rigorous third-party risk assessments will be essential, ensuring both internal and vendor controls are evaluated.

- **Cloud Privacy Enhancements**

As businesses migrate to the cloud, SOC 2 and SOC 3 updates will emphasize strong data privacy measures to protect personal and sensitive information.

- **Operational Transparency**

Updates will promote operational transparency, encouraging organizations to disclose more about their security policies and incident response strategies to build trust and accountability.

### **Addressing the Evolving Threat Landscape**

The shifting landscape of cybersecurity threats demands that organizations remain vigilant and adaptive. With cyberattacks becoming increasingly sophisticated, the updates to the SOC frameworks illustrate a commitment to evolving alongside these threats. By reinforcing the importance of risk management and third-party security, organizations can better protect themselves against malicious actors and safeguard their data integrity.

### **Conclusion**

The anticipated updates to the SOC 2 and SOC 3 frameworks underscore a significant shift in how organizations approach security, risk management, and data privacy. As these frameworks evolve, they will play a crucial role in helping organizations navigate the complexities of an increasingly interconnected world. By prioritizing operational transparency and a robust risk management strategy, organizations can not only enhance their security posture but also establish a foundation of trust with their customers and stakeholders. Embracing these updates is not just about compliance; it is about fostering a culture of security and resilience that can withstand the challenges of the future.

---



# Strategies and Tools

---

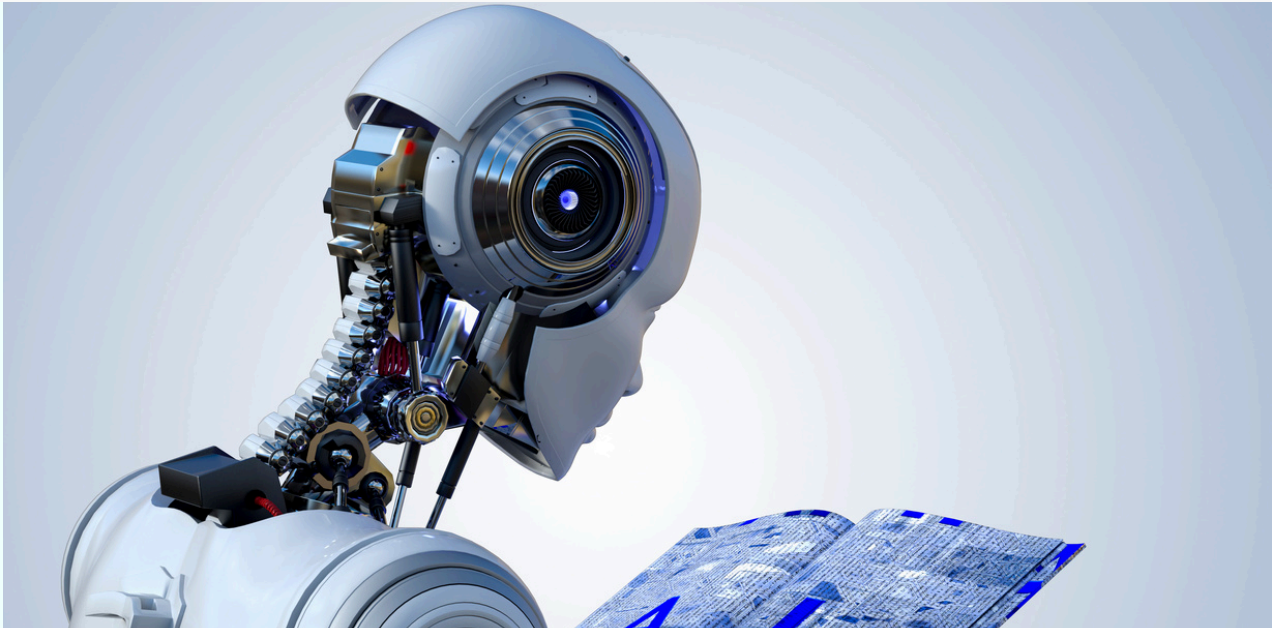




---

# Artificial Intelligence & Machine Learning

-Venkat G



Automated compliance tools have taken center stage, streamlining and easing complex procedures, dramatically reducing the potential for oversight errors.

AI-powered tools can analyze financial statements and identify trends, anomalies, and potential risks in real time. This assists accountants in making more accurate financial assessments and take strategic decisions.

AI, machine learning (ML), and software are transforming industries across the globe, creating significant shifts in how businesses operate, innovate, and serve their customers.

**Here are some ways these technologies are reshaping industries:**

- **Healthcare-** AI Diagnostics, Personalized treatment and drug discovery
- **Finance-** Fraud detection, Algorithmic trading, Risk Assessment
- **Retail-** Personalization. Inventory management and customer service
- **Manufacturing-** Predictive maintenance, Automation, supply chain optimization

- 
- **Transportation-** Autonomous vehicles, Traffic optimization, Predictive Analytics
  - **Entertainment Media-** Content creation, Recommendation systems, Audience insights
  - **Energy-** Smart grids, Energy consumption forecasting, Renewable Energy
  - **Education-** Adaptive Learning, Automated Grading, AI Tutors,
  - **Legal and Compliance-** Document Review and Analysis, Predictive Legal Analytics, Contract management
  - **Agriculture-** Precision farming, Pest and Disease prediction, Automated harvesting
  - **Human Resources-** Talent Acquisition, Employee Sentiment Analysis, Workplace efficiency
  - **Security-** Cybersecurity, Facial recognition, Threat intelligence

#### **Key Challenges and Considerations:**

- **Bias:** AI and ML models are only as good as the data they are trained on. If the data contains biases, the models can produce biased outcomes, leading to unfair or discriminatory results.
- **Data Privacy:** The collection and analysis of large amounts of personal data raise concerns about privacy and security, especially in sensitive sectors like healthcare and finance.
- **Job Displacement:** As automation increases, there is concern about job losses, especially in industries like manufacturing and customer service.
- **Regulation:** Governments are grappling with how to regulate AI technologies to ensure ethical use and prevent misuse, especially in areas like surveillance and decision-making.

In conclusion, AI, ML, and software are accelerating innovation and transforming industries by improving efficiency, enhancing personalization, reducing costs, and enabling new business models. However, these changes also come with challenges that need to be addressed responsibly to ensure equitable and ethical outcomes for society.

---

# Mandatory Penetration Testing: A Critical Requirement for Cyber Resilience

-Sidhartha Sharma



In today's rapidly evolving cyber security landscape, penetration testing has shifted from being a best practice to a mandatory requirement for many organizations. With increasing regulatory compliance mandates and the rising sophistication of cyber threats, organizations must adopt regular assessments to identify and mitigate vulnerabilities in their critical systems.

## Why Penetration Testing is Mandatory?

1. Regulatory Compliance Standards such as PCI-DSS, ISO 27001, HIPAA, and SOC 2 mandate periodic security testing to ensure systems remain resilient against cyber threats. Failing to conduct penetration tests may result in compliance violations and potential fines.
2. Proactive Threat Mitigation Regular testing helps organizations uncover security weaknesses before malicious actors exploit them, reducing the risk of data breaches, financial loss, and reputational damage.
3. Strengthening Incident Response Pentesting not only helps in identifying vulnerabilities but also enhances incident response readiness, ensuring organizations can detect, contain, and remediate security threats effectively.
4. Securing Critical Systems As cyber attacks grow more sophisticated,



---

organizations must prioritize proactive defense strategies. A well-executed penetration test provides actionable insights to fortify critical infrastructure against real-world attack scenarios.

### **VAPT Audit Process**



### **How Riskpro Can Help**

Riskpro empowers organizations by offering comprehensive penetration testing and guidance that ensures the security of critical systems. We provide rigorous assessments and tailored recommendations to strengthen your defenses against evolving threats.

By partnering with Riskpro, you invest in a proactive cyber security approach that aligns with emerging industry standards, safeguarding your operational integrity and strengthening your overall security posture in increasingly complex digital landscapes

# The Importance of AI Auditing: Ensuring Transparency and Compliance

-Sucheta Upendra



## Why do AI systems need auditing?

It was an energy-packed week at TAI (Technology and AI), a leading start-up known for innovative AI solutions. The company recently developed AI-driven tools that promised to transform customer engagement through personalized interactions and actionable insights.

The prototype was ready, and the product team was raring to go. However, the management decided to conduct an AI audit to address concerns about ethical behavior, transparency, and compliance with legal standards.

The development team's perplexity led them to their 'go-to' GenAI tool for insights on this topic.

## One more audit?

After all, AI-based systems are designed to increase productivity and make our

---

lives easier. The right AI tool would improve businesses exponentially. We also comply with industry best practices for information security and data privacy. Why do we need an additional audit?

### **AI Audits**

AI auditing is a comprehensive process that examines key components of AI systems: policies, data, algorithm, and outcome auditing.

**Policies:** The first step is to check if the organization has an AI policy based on ethics, compliance, and technology risks. Does it consider the different types of risks AI systems may pose and provide guidance on controls to avoid and mitigate the risks?

**Data Auditing:** This step involves reviewing the data used by AI systems to ensure it is high-quality - accurate, complete, and unbiased.

For TAI, this meant

- Checking the customer data collection processes and ensuring that the collection, processing, and storage complied with the requirements on transparency and consent.
- Ensuring that the data represented diverse demographics
- Security of the data collected and compliance with data privacy practices

**Algorithm Auditing:** This involves scrutinizing the algorithms to ensure they function as designed and are free from bias or errors. The auditors delve into the AI algorithms' logic and parameters to identify potential issues that could lead to biased recommendations. It is recommended that the AI development team implement techniques to explain AI-driven decisions, enhancing trust and compliance with regulatory requirements.

For TAI, it also involved confirming if AI algorithms could unintentionally favour specific customer demographics.

**Outcome Auditing:** The final step is to evaluate the AI system's results to ensure they are accurate, fair, and consistent with expected outcomes. For TAI, this meant comparing the AI-generated recommendations with baseline standards and checking for deviations or anomalies.

### **Baseline standards for the audit**

Auditing AI-based systems involves ensuring they operate ethically, transparently, and in compliance with relevant standards and regulations, such



---

as ISO 42001 and the EU AI Act.

- **ISO 42001:** This standard focuses on building an AI management system, emphasizing on controls to be implemented by AI developers and deployers.
- **EU AI Act:** This regulation helps classify AI systems based on risk and aims to ensure their safety and trustworthiness by setting rules for their development and deployment. It includes provisions for transparency, accountability, and human oversight.

### **The Impact of AI Auditing**

The AI audit at TAI would not only ensure compliance with data privacy regulations but also help build trust among stakeholders by clarifying the AI system's decision-making processes.

### **Conclusion**

By identifying and mitigating risks such as biases or algorithm errors, TAI prevented potential issues that could have led to significant reputation or financial damage.

As AI continues to transform industries, the importance of auditing these systems cannot be overstated. Organizations like TAI can harness AI's full potential while maintaining trust and reliability by ensuring that AI systems operate as intended, are transparent, and comply with ethical and legal standards.

(\*: Disclaimer: The company – Technology and AI - TAI, and events depicted above are fictitious. No association with any real company, or events is intended or should be inferred.)

---

# Strengthening Financial Systems Against Illicit Activities: The Imperative of Anti-Money Laundering (AML)

-Ekta Gada



In an increasingly interconnected world, the financial system not only facilitates global trade and economic growth but can also serve as a conduit for illegal activities, particularly money laundering. Anti-money laundering (AML) efforts are crucial as criminals exploit financial systems to legitimize funds obtained from crime. This article highlights the importance of robust AML frameworks, emerging trends, and the need for collaboration among stakeholders.

## **Understanding Money Laundering**

Money laundering transforms illegal gains into seemingly legitimate money through methods like layering (hiding the source of funds) and integration (reintroducing laundered money into the economy). The consequences are far-reaching, undermining the integrity of financial institutions and facilitating organized crime.

---

## The Global AML Landscape

Over the years, governments and international organizations have established comprehensive AML regulations. The Financial Action Task Force (FATF) sets the global standards for AML and combating the financing of terrorism (CFT). Countries failing to comply risk sanctions and reputational damage.

## Key Components of Effective AML Programs

- **Risk Assessment:** Financial institutions must identify vulnerabilities through thorough risk assessments to tailor AML strategies.
- **Customer Due Diligence (CDD):** Robust CDD measures, including verifying customer identities and monitoring transactions for suspicious activity, are essential.
- **Transaction Monitoring:** Advanced analytics and real-time monitoring can flag suspicious activities, with machine learning enhancing accuracy and efficiency.
- **Regulatory Compliance:** Adhering to local and international regulations is essential for effective AML efforts.
- **Reporting and Collaboration:** Timely reporting of suspicious activities to authorities, along with collaboration between financial institutions and law enforcement, is critical for effective AML responses.

## The Role of Technology

Technology plays a crucial role in AML strategies. Innovations like artificial intelligence (AI) and blockchain are transforming compliance practices by automating tasks and improving transaction traceability. While blockchain enhances transparency, the anonymity provided by certain cryptocurrencies poses new challenges, necessitating updated regulatory measures.

## Conclusion: A Collective Responsibility

Combating money laundering requires a multi-faceted approach. Collaboration among financial institutions, governments, and international organizations is vital for building resilient financial systems. By investing in technology and committing to ethical practices, stakeholders can strengthen AML efforts. A proactive stance against money laundering is essential for safeguarding financial system integrity, fostering trust in economic activities, and creating a secure global financial environment for all.

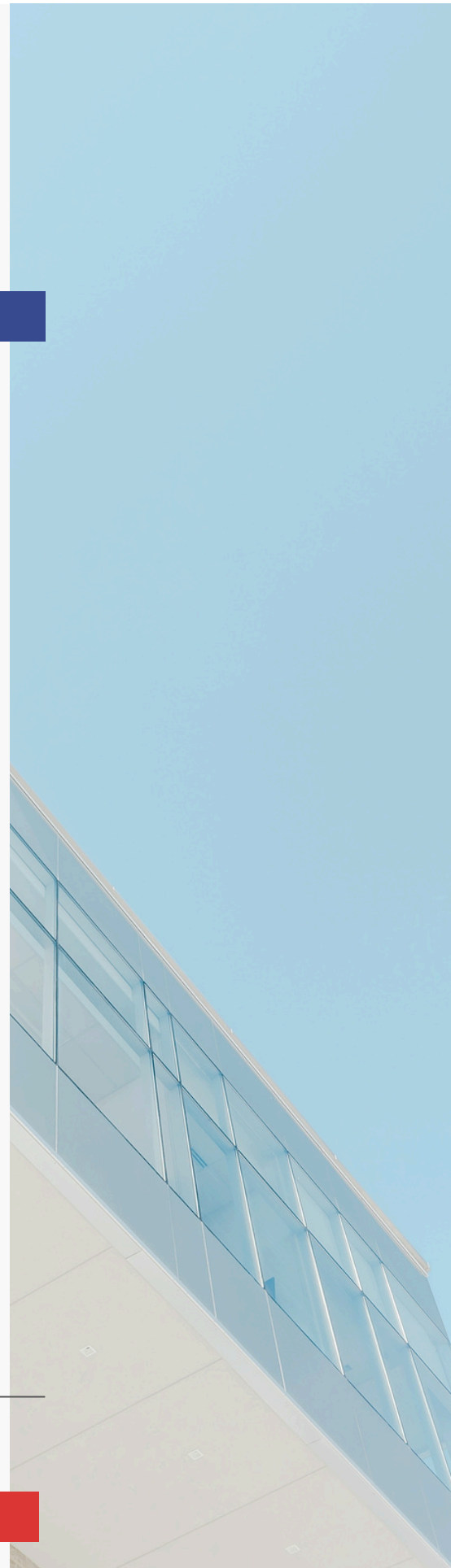


---



# Regulatory Updates

---



---

# Global Risk Management Landscape: Key Regulatory Developments

-Sonakshi Sinha



The regulatory landscape continues to evolve, presenting organizations with complex compliance obligations that require strategic realignment of risk management frameworks. Key developments demand immediate attention from privacy and compliance professionals.

## **European Union Updates:**

- **DORA (Jan 2025):** Enforces stringent ICT risk management for financial entities, emphasizing third-party risk management and incident response.
- **AI Act (Aug 2025):** Introduces tiered risk classification, impacting AI deployment strategies.
- **CSDDD (2027):** Extends privacy and data protection into supply chains, requiring enhanced due diligence.

## **U.S. Regulatory Evolution:**

- **Anti-Money Laundering Reforms:** Increasing scrutiny necessitates enhanced risk assessment methodologies.

- 
- **AI Regulation:** Organizations must prepare for fragmented federal and agency-specific guidelines on transparency and data protection.
  - **ADPPA:** Establishes a federal privacy framework, replacing state laws and introducing data minimization, consumer rights management, and enhanced security controls for large data holders.

#### **Asia-Pacific Compliance Landscape:**

- **ASEAN Medical Device Directive:** Requires risk-based data protection for medical devices.
- **India's AI Framework:** Emphasizes ethical AI principles and privacy-by-design compliance.

#### **Strategic Compliance Priorities:**

- Cross-jurisdictional monitoring for evolving regulations.
- Enhanced risk assessment methodologies and third-party risk management.
- Proactive compliance programs addressing future regulatory shifts.

#### **Global Data Protection Considerations:**

- **Regulatory Convergence:** GDPR remains the global privacy benchmark, with expanding U.S. state laws and emerging frameworks in India.
- **Technical Controls:** Organizations should integrate cryptographic security, de-identification frameworks, and privacy-enhancing technologies.
- **Cross-Border Data Governance:** Data transfer impact assessments, partner due diligence, and contractual controls are essential for compliance.

**Implementation Strategy:** Organizations must develop jurisdiction-specific roadmaps, integrate privacy-by-design principles, and establish continuous compliance monitoring. Aligning privacy controls with broader information security frameworks ensures resilience in an evolving regulatory environment.

---

# 2024 Best practices in compliance and upcoming changes in 2025

-Suchitra Muley



Adhering to constantly changing rules is a difficult but unavoidable duty in the dynamic world of corporate governance. The difficulties presented by the quickly evolving regulatory landscape are recognized by senior management, which is also in charge of compliance management. In order to solve these issues, particularly for medium-sized and big corporations, we present five best practices for compliance management systems (CMS).

The importance of compliance is more than ever in the fast-paced corporate world of today. Organizations must continue to be flexible and proactive in order to stay out of trouble with the law as rules become more frequent and complicated. Avoiding fines is only one benefit of compliance; it also helps businesses keep the confidence of investors, consumers, and authorities.

## **Best Practices for Compliance**

- Stay Informed About Regulatory Change
- Foster a Strong Compliance Culture
- Implement Robust Internal Controls



- 
- Ensure Effective Reporting Mechanisms
  - Perform Regular Risk Assessment

### **Upcoming Changes to Watch For**

Long-term success depends on future-proofing your compliance program as regulatory environments change and companies encounter more complicated problems. Nowadays, compliance involves more than just following the law; it also involves staying ahead of trends, foreseeing shifts, and adjusting to new risks in a setting that is changing quickly.

Here's how organizations can future-proof their compliance strategies: Future-proofing compliance involves proactive preparation for regulatory changes rather than only responding to them. Businesses may overcome today's obstacles and withstand the complexity of tomorrow's compliance environment by establishing a strong compliance culture, utilizing technology, maintaining agility, and concentrating on long-term risk management. In addition to reducing legal risks, making sure your company is ready for the future of compliance can improve consumer trust, boost brand recognition, and put you in a position for long-term success.

### **Techniques for Handling Compliance in the Future**

Organizations must take a proactive stance in order to handle these issues and take advantage of new trends:

#### **Encourage a Culture of Compliance:**

Clear communication, frequent training, and leadership support are necessary to establish a compliance culture. Workers should be aware of how crucial compliance is and how they contribute to maintaining standards.

#### **Work Together with Professionals:**

Organizations may traverse difficult regulatory environments by collaborating with technology suppliers and compliance specialists. These professionals simplify compliance efforts with their particular expertise and tools.

#### **Adopt a Risk-Based Approach:**

Focusing on high-risk areas allows organizations to allocate resources more effectively. Regular risk assessments ensure that compliance efforts remain

Make Use of Technology Investing in cloud-based compliance technologies, blockchain, and artificial intelligence (AI) may lower risks and increase efficiency.

These technologies are appropriate for businesses of all sizes since they allow for scalability.



### **Conclusion**

Building trust, controlling risks, and guaranteeing an organization's long-term performance are all goals of compliance, which goes beyond just fulfilling legal obligations. Organizations may confidently traverse the ever-increasing complexity of compliance by cultivating a culture of compliance, keeping up with evolving requirements, and utilizing technology to optimize procedures.

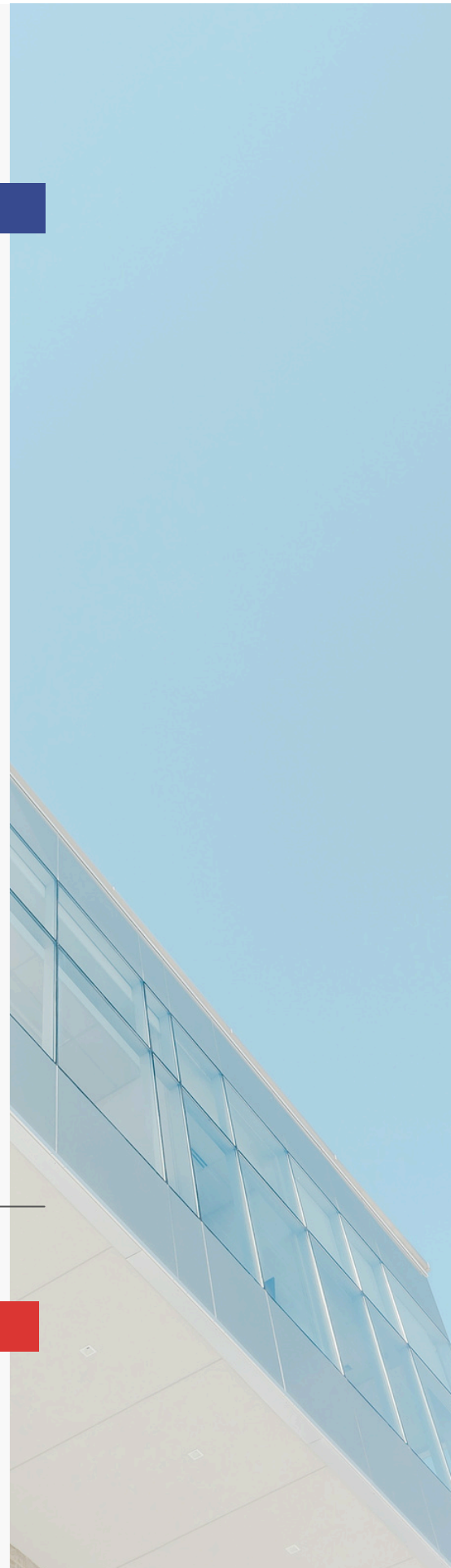
The changes on the horizon present both challenges and opportunities for businesses to improve their compliance practices. Keeping an eye on these trends, while taking proactive steps now, will help organizations mitigate risks and stay ahead of the curve.

---



# **Risk Management Around the World**

---



---

# Global Risk Management: A Comparative Analysis of Risk Landscapes Across Regions

-Sanket Prabhu



In today's interconnected world, risk management is a crucial aspect of business, government, and individual decision-making. From natural disasters to financial crises, organizations and nations must navigate diverse risks shaped by economic, cultural, and regulatory factors. Understanding global risk management practices provides insight into best practices, challenges, and opportunities in mitigating threats.

**The Importance of Risk Management** Risk management involves identifying, assessing, and prioritizing risks to minimize potential harm. Its significance has grown due to global uncertainties like climate change, cyber threats, economic instability, and geopolitical tensions. Governments and businesses worldwide are increasingly investing in proactive risk strategies to safeguard assets and operations.

## **Regional Approaches to Risk Management**

- **North America:** A strong legal framework guides risk management, with regulations like the Sarbanes-Oxley Act ensuring corporate governance and cybersecurity investments protecting organizations from digital threats.



- **Europe:** A mix of traditional and modern practices shapes risk management. EU regulations such as Basel III and Solvency II enhance financial sector stability, while sustainability concerns drive environmental risk strategies.
- **Asia:** Japan integrates risk management into daily operations through the "Kaizen" approach. China focuses on financial and environmental risks, while India adopts global standards to address corruption, natural disasters, and market volatility.
- **Latin America:** Political instability, economic fluctuations, and natural disasters shape risk management. Businesses employ flexible frameworks to navigate inflation, social movements, and financial crises.
- **Africa:** Risk management tackles political risk, corruption, and climate-related challenges. Digital finance innovations and sustainable practices are becoming key strategies in managing financial and environmental risks.

Risk is a constant factor in every region, presenting unique challenges for businesses, governments, and individuals. Understanding these risks is crucial for informed decision-making. This article provides an overview of risk landscapes in three key regions: Asia-Pacific, Europe, and the Americas.

### **Asia-Pacific: Growth Amid Complex Risks**

The Asia-Pacific (APAC) region, home to rapidly expanding economies like China, India, and Southeast Asia, faces diverse risks:

- **Economic Risks:** Market volatility, exchange rate fluctuations, and trade tensions, particularly between the U.S. and China, impact businesses. Policies like China's "Made in China 2025" affect global supply chains.
- **Political & Regulatory Risks:** Regulatory unpredictability, particularly in China, and political instability in Southeast Asia add uncertainty for investors.
- **Environmental Risks:** High exposure to natural disasters like tsunamis and typhoons, climate change threats, and rising sea levels endanger coastal cities and agriculture.

### **Europe: Geopolitical Uncertainty and Economic Challenges**

Europe faces risks driven by economic, geopolitical, and environmental factors:

- **Economic Risks:** Eurozone stability, Brexit aftershocks, and regulatory compliance costs under GDPR and MiFID II create financial challenges.
- **Political & Geopolitical Risks:** Brexit uncertainty, Russian influence in Eastern Europe, and rising populism contribute to political instability.
- **Environmental & Social Risks:** The European Green Deal's transition to sustainability imposes economic burdens, while demographic shifts and migration pose social challenges.

---

### **The Americas: Balancing Growth and Uncertainty**

North and South America experience varied risks across economic, political, and environmental domains:

- **Economic Risks:** U.S. trade policies, inflation, and tax system changes affect stability, while South America faces inflation, currency volatility, and governance issues.
- **Political & Geopolitical Risks:** Political instability, corruption, and organized crime in Latin America, along with shifting U.S. trade policies, impact business operations.
- **Environmental Risks:** Hurricanes, deforestation in the Amazon, and climate change threaten infrastructure, agriculture, and economic stability.

**Challenges and Future Trends** Common global challenges include increasing risk complexity, cybersecurity threats, and a shortage of skilled professionals, particularly in emerging markets. The future of risk management will leverage artificial intelligence and machine learning for predictive analytics and real-time monitoring. Additionally, the rise of environmental, social, and governance (ESG) considerations will drive long-term sustainability efforts.

### **Conclusion: Navigating Global Risks**

Each region faces distinct risks—APAC grapples with economic volatility and natural disasters, Europe contends with geopolitical shifts and regulatory challenges, while the Americas face political and environmental uncertainties. Organizations must assess regional risks to develop effective strategies for navigating today's complex global landscape. In conclusion, while risk management approaches vary across regions, the need for proactive and comprehensive strategies is universal. As globalization continues, effective risk management will be essential in ensuring stability and resilience worldwide.

# Collaboration Efforts in International Risk Management

-Sanket Prabhu



In an interconnected world, risks such as financial instability, cyber threats, climate change, and pandemics transcend borders, necessitating global collaboration. No single nation can effectively address these complex challenges alone. International cooperation is crucial in fostering resilience and mitigating global risks.

## **Key Areas of International Collaboration:**

- **Climate Change and Environmental Risks-** Global warming poses a severe threat, requiring collective action. The Paris Agreement, adopted in 2015, unites nearly 200 countries in reducing greenhouse gas emissions. Organizations like the Carbon Disclosure Project (CDP) and Global Reporting Initiative (GRI) promote corporate environmental responsibility.
- **Public Health and Pandemic Preparedness-** The COVID-19 pandemic highlighted the need for international health cooperation. The World Health Organization (WHO) and the Coalition for Epidemic Preparedness Innovations (CEPI) coordinate global responses,

---

while public-private partnerships accelerate vaccine development and distribution.

- **Cybersecurity and Digital Risks-** Cyber threats are increasing globally, necessitating cross-border collaboration. Organizations such as the European Union Agency for Cybersecurity (ENISA) and the Global Forum on Cyber Expertise (GFCE) work on developing cybersecurity frameworks and enhancing threat intelligence sharing.
- **Financial Risk and Economic Stability-** Economic crises, like the 2008 financial meltdown, demonstrate the global nature of financial risks. Institutions such as the International Monetary Fund (IMF), World Bank, and Basel Committee on Banking Supervision promote stability through financial regulations and assistance programs.
- **Geopolitical and Political Risks-** Trade disputes, conflicts, and political instability require diplomatic efforts. The United Nations (UN), European Union (EU), and World Trade Organization (WTO) facilitate dialogue, peacekeeping, and trade regulations to mitigate geopolitical risks.

### **Challenges and the Future of Global Risk Management**

While collaboration is essential, challenges such as differing national priorities, political tensions, and resource disparities hinder progress. Adaptability and continuous framework updates are necessary to address evolving risks. The integration of artificial intelligence and big data offers promising advancements in monitoring and mitigating global threats.

### **Conclusion**

International collaboration in risk management is imperative for addressing global challenges. Governments, businesses, and organizations must work together to build a resilient and secure world, leveraging cooperation to navigate risks effectively and safeguard future generations.

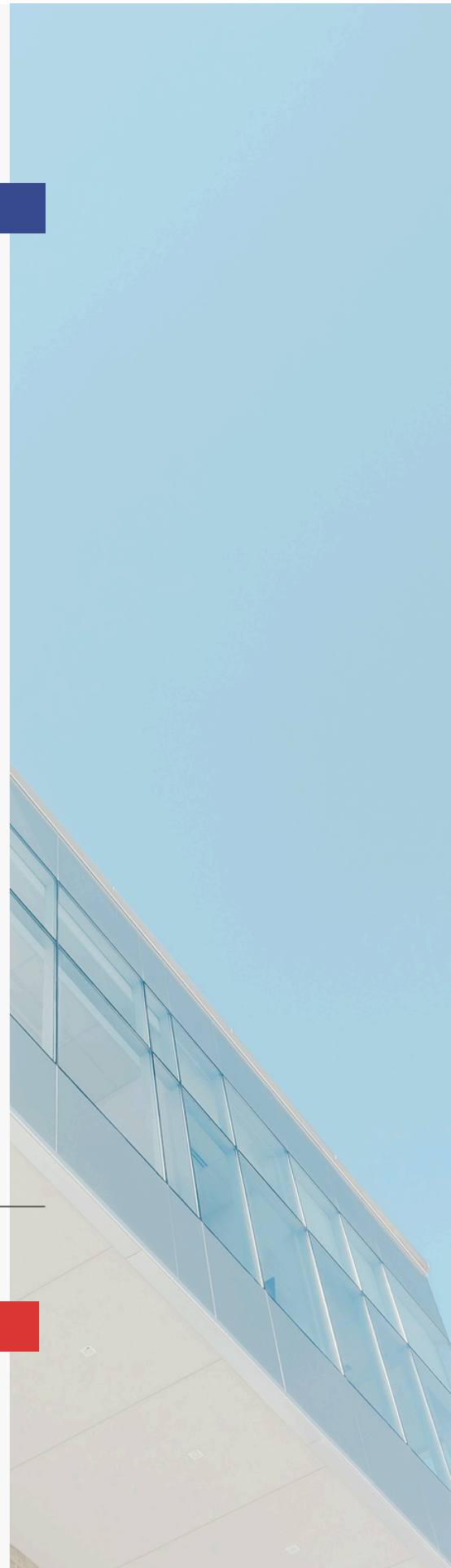


---



# **Sustainability & GRC Integration**

---



---

# Holistic Risk Management: Integrating Governance, Risk, and Compliance for Enhanced Decision-Making

-Raghvendra Mishra and Ekta Gada



In today's complex business landscape, organizations face an array of risks that can threaten their objectives and overall success. As these threats become increasingly interconnected, adopting a holistic risk management approach is essential. This method enables organizations to identify, quantify, and manage risks comprehensively, rather than in isolation. By converging Governance, Risk, and Compliance (GRC) functions, organizations can leverage integrated platforms that provide a unified view of risk, compliance, and governance activities, ultimately enhancing decision-making and operational efficiency.

---

### **Understanding Holistic Risk Management**

Holistic risk management is defined as the process through which an organization identifies and quantifies all threats to its objectives, managing these threats within its existing management framework. This approach emphasizes a broad understanding of risk across the entire organization, rather than focusing solely on specific components. By adopting this comprehensive perspective, organizations can better navigate the complexities of risk in a large-scale environment where business risks are often challenging to control.

One of the key advantages of holistic risk management is its ability to break down traditional risk silos. In many organizations, risk management efforts are compartmentalized, leading to a fragmented view of potential threats. Holistic risk management encourages a more integrated perspective, allowing organizations to assess risks across different departments and functions. This integration is particularly important in today's rapidly evolving business landscape, where the emergence of technologies like artificial intelligence (AI) presents both opportunities and challenges.

### **The Role of AI in Holistic Risk Management**

AI plays a significant role in enhancing holistic risk management by providing tools and insights that facilitate end-to-end business threat assessments. With AI, organizations can analyze vast amounts of data, identify patterns, and predict potential risks more accurately. This capability not only improves risk assessment but also empowers organizations to develop proactive strategies for risk mitigation.

For instance, AI-driven analytics can help organizations understand their operational risk profile better, allowing leadership to define their risk appetite and craft effective risk mitigation strategies. By harnessing AI, organizations can streamline their risk management processes, making them more efficient and responsive to emerging threats.

### **The Importance of Organizational Structure**

Another essential component of holistic risk management is the organizational structure. An organization that has a clear understanding of its risk profile across various silos is better equipped to implement policies and procedures that address potential risks. This understanding fosters collaboration among different departments, ensuring that everyone is aligned in their approach to risk management.

---

Moreover, a well-defined organizational structure supports the integration of GRC functions. By aligning governance, risk, and compliance activities, organizations can create a cohesive framework that enhances decision-making. This unified approach not only improves operational efficiency but also strengthens the organization's resilience against risks.

### **Conclusion**

As organizations navigate the complexities of modern business, adopting a holistic risk management approach is becoming increasingly vital. By integrating GRC functions and leveraging technologies like AI, organizations can achieve a unified view of risk, compliance, and governance activities. This comprehensive perspective enhances decision-making and operational efficiency, enabling organizations to respond more effectively to the challenges they face.

In conclusion, holistic risk management is not just a strategy; it is a necessity for organizations aiming to thrive in an unpredictable environment. By embracing this approach, organizations can better protect their objectives and position themselves for sustainable success in the future.



---

# What does a Sustainability Partner look like?

- Casper Abraham



The word “sustainability” is over-used. As is “green”. To this extent we now even have a word to describe this, “green-washing”. Just because you have used the word green in your brand name, logo or tag-line it does NOT make your business and supplies green. If your advertising, marketing and sales collateral is dominantly in the colour green, it still does NOT make your business nor supplies green. Getting some sort of “green certification” or “green-rating” does move the needle in the right direction – and the world does recognize effort and attempt to make your business and supplies green. It’s a journey and a good start.

Some justifiable claim of being “sustainable” or green” starts with transparency and disclosure. From investors and stake-holders and your top-management down to the grass-roots of your business your your supplies. Other attempted awareness, effort, activity and outcome associated words or sentences can include; “reduction in carbon foot print”, “quantifying all your carbon di-oxide equivalent emissions”, “net-zero target, achievements & gaps”, “transition away from fossil-fuels”, “adaptation of or replacement with renewable energy”, aligning business and supplies to UN SDG (United Nations Sustainable Development Goals).

---

While initial “checkbox” activity and meeting regulatory controls is important and gets you started - It’s a journey and you can attempt to achieve this over 5 years setting yourself a 5-phase Green Maturity Model.

Every country now has some regulatory protections that are linked to Climate change, climate risk, risks to your industry or from your industry because of environmental considerations, social issues, ethics and governance which have many 3-letter words, have different emphasis and looks different in its many avatars.

These include the mandatory – in India - BRSR (for top-1000 SEBI listed firms) Business Responsibility and Sustainability Reporting every year. While it’s again a “checkbox” submission – it can be picked up seriously not just if you are a listed business in India but any medium to large firm as the “intent” it is rooted in is the same.

The “sustainability adherence intent” is about 40 to 200 parameters that cuts across all industry and all business verticals, and business horizontals and functions across any size of central, state, public or private, social or any enterprise.

These “sustainability-intent-90” (we can assume an average of these many parameters that will set you on the path whether you are in the US, Europe, Asia-Pacific, Africa, Middle East, China, Japan or other geographies. There are many such as GRI, CDP, TCFD, MCI index, Ecovadis, CSRD ESRS 1 and 2, CBAM, ISO standards, NIST frameworks all need you have control on these “sustainability-intent-90”.

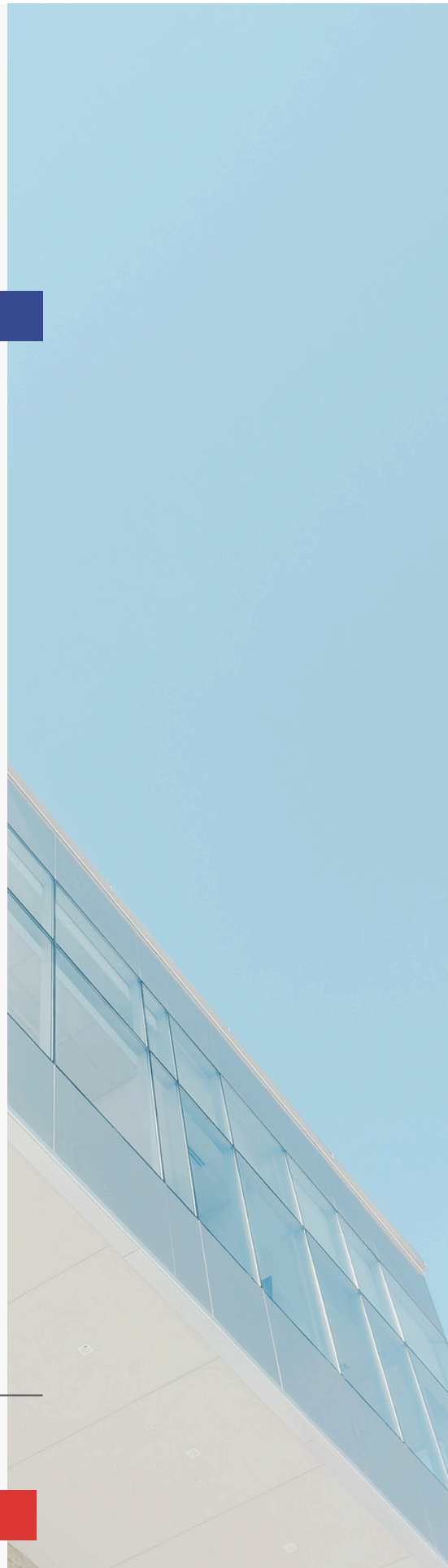
The “sustainability-intent-90” now broadly included in say ESG (Environment Social & Governance). About 30 parameters in each of Environment pillar, Social pillar and Governance pillars. Earlier CSR and BRR in India is morphing into this common set of “sustainability-intent-90” parameters. While GRC has traction in the regulatory community, Governance & Compliance is rolled into ESG. Risk management is always a part of any serious regulatory concern. An important mechanism to manage these “sustainability-intent-90” could be with a deployment of a standard ERM (Enterprise-Risk-Management) that lists all your risk into a risk-register. Having identified and ranked, measure, monitor and manage each of them. Put in place gap reduction strategies, controls and be ready for any business model, reporting, market or regulatory requirement that you are confronted with today and in the future. You will be ready. Talk to us at Riskpro as your “Sustainability Partner” we have our Quality Supply Chain to meet any needs by any industry in any part of the world out of India.

---



# Company Highlights

---



---

# Riskpro Growth:

Our journey has been one of resilience, innovation, and unwavering commitment to excellence. From humble beginnings to a thriving enterprise, our company's growth is a testament to our vision, teamwork, and adaptability in an ever-evolving industry. With each milestone, we continue to push boundaries, embrace new opportunities, and set higher benchmarks for success. This page celebrates our progress, our people, and the future we are building together.

**10.43%**

## Revenue Growth in 2024:

Our consistent revenue growth reflects our commitment to excellence and innovation. As we scale new heights, we remain focused on delivering value to our customers and stakeholders."

**12.77%**

## Partner growth in 2024:

"Our expanding network of partners showcases our strong collaborations and market trust. Together, we are driving innovation and creating greater value for our customers."

**16.13%**

## Company growth in 2024:

Our growing team is a testament to our dynamic work culture and commitment to excellence. We continue to invest in our people, empowering them to drive innovation and success.

**13.4%**

## Customer growth in 2024:

Our expanding customer base reflects the trust and confidence in our solutions. We remain dedicated to delivering exceptional value and building lasting relationships."

# Partnerships at Riskpro

-Abigail Crasto

## **Riskpro's Expanding Strategic Partnerships: Driving Mutual Growth in Compliance & Risk Consulting**

In the ever-evolving landscape of compliance, risk management, and cybersecurity, collaboration is key to delivering comprehensive solutions. At Riskpro, a leading compliance and risk consulting firm, we have always prioritized strategic partnerships as a core part of our growth strategy. By aligning with industry experts in cybersecurity, IT infosec, data privacy, ISO certification, cloud security, VCISO, VAPT, automation, GRC technology, CA, and audit, we ensure that our clients receive best-in-class services tailored to their needs.

## **A Growing Network of Trusted Partners**

2024 has been a landmark year for Riskpro, with the addition of 50 new strategic partners across diverse domains such as data privacy, ISO 27001 certification, cybersecurity, and automation. This expansion is not just about increasing numbers but about strengthening our capabilities and enhancing the value we bring to our clients.

Our strategic alliances are built on mutual profitability, ensuring that both Riskpro and our partners benefit from a symbiotic relationship. As we bring business to our partners through our vast client base, they, in turn, open new avenues for us by leveraging their expertise and networks. This collaborative model has proven to be a win-win, driving significant business for all stakeholders involved.

## **Why Our Partnerships Matter**

- **Comprehensive Service Offerings:** Through our partnerships, we provide end-to-end solutions, from compliance assessments to advanced cybersecurity measures.
- **Enhanced Business Growth:** The cross-referral model ensures steady business flow, allowing all partners to scale and reach new markets.
- **Innovation and Automation:** By working with cutting-edge technology providers, we integrate automation and GRC solutions that streamline risk management processes.



- **Industry Compliance Expertise:**

Our partnerships in ISO certification and data privacy ensure that clients remain compliant with evolving global regulations such as GDPR, CCPA, and ISO 27001.

- **Cybersecurity Reinforcement:**

With rising cyber threats, our collaborations with VAPT and cloud security firms help businesses safeguard their digital assets.

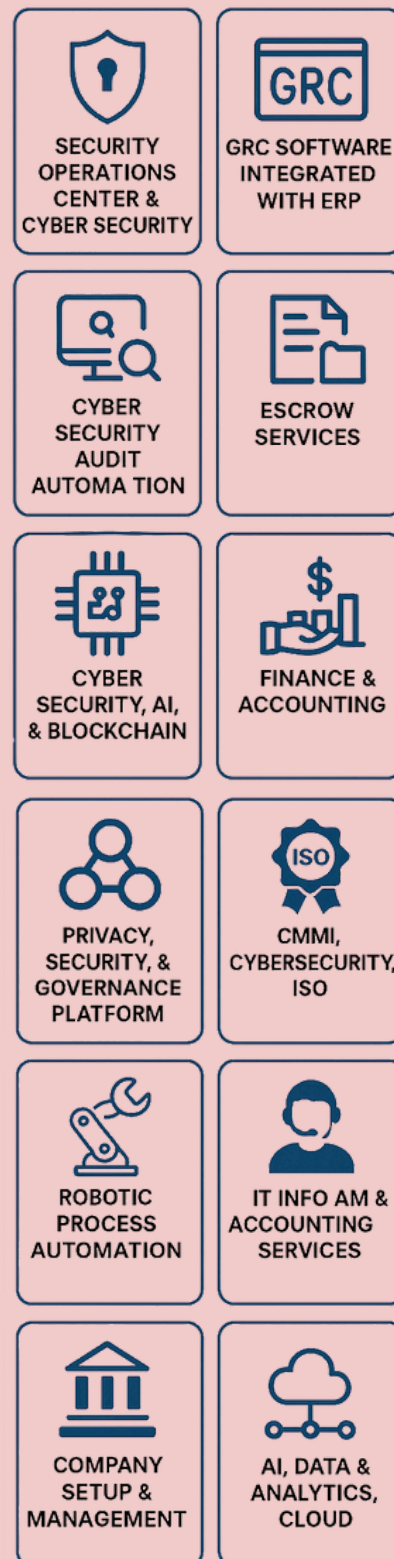
### Looking Ahead: Expanding Opportunities

At Riskpro, we are always on the lookout for new partners who can add value to our ecosystem. As compliance and risk landscapes continue to evolve, we remain committed to expanding our network, enhancing our service offerings, and driving **profitability for both our partners and ourselves**.

Whether you're a cybersecurity expert, an automation specialist, or a compliance consultant, partnering with Riskpro means becoming part of a **dynamic and growing ecosystem** that thrives on collaboration, trust, and business growth.

If you're interested in exploring partnership opportunities with us, reach out today and let's build a future of secure, compliant, and efficient business operations together.

**New Partners added have been in the areas of -**



At Riskpro, we are committed to fostering partnerships that are mutually profitable and beneficial. To achieve this, we focus on several key strategies:

- **Ethical Business Practices:** We firmly believe in fair and ethical business practices when dealing with our clients, people, and associates. This commitment to integrity ensures that all parties can rely on us to solve problems, answer questions, and provide support, fostering trust and long-term collaboration.
- **Clear Roles and Responsibilities:** Establishing well-defined roles and responsibilities is essential for effective collaboration. By clearly outlining each partner's scope of work and obligations, we ensure accountability and prevent misunderstandings that could lead to unnecessary risks.
- **Regular Performance Evaluation:** We prioritize ongoing evaluation of both individual and collective contributions toward our partnerships. By openly discussing strengths, weaknesses, and areas for improvement, we enhance our collaborative practices and encourage a culture of continuous learning and improvement.

- **Competitive and Transparent Pricing:** Our fees are highly competitive and transparent, often well below those of larger consulting firms. This approach allows us to deliver cost-effective solutions, ensuring that our partners receive maximum value without compromising on quality.
- **Leveraging Expertise and Alliances:** With a management team possessing over 500 years of collective experience in business, financial, and technology risk, and strategic alliances with leading consulting firms across India, we bring a vast pool of expertise to our partnerships. This depth of knowledge enables us to provide practical and implementable solutions tailored to our partners' needs.
- **Innovative Service Models:** We offer unique service models, such as "Risk 365," which provides a flat-fee pricing structure for a wide range of risk and compliance services.

By integrating these strategies into our partnership approach, Riskpro ensures that collaborations are not only profitable but also built on a foundation of trust, transparency, and shared success.

# Highlights from 2024 Conferences, Webinars, and Workshops

-Ekta Gada

As we step into 2025, it's essential to reflect on the pivotal insights and developments that transpired during the various conferences, webinars, and workshops hosted by RiskPro throughout 2024. This year's events showcased the latest trends, strategies, and technologies in risk management, attracting participants from diverse sectors including finance, insurance, healthcare, and cybersecurity.

## **Keynote Sessions and Expert Panels**

One of the standout features of our conferences was the array of keynote speeches and expert panels. Notable speakers from industry-leading organizations shared their expertise on pressing topics, including regulatory challenges, the integration of AI in risk assessment, and the evolving landscape of cyber threats. The panel discussions fostered rich dialogue and provided attendees with actionable insights, helping them navigate the complexities of today's risk environment.

## **Workshops: Hands-On Learning**

The interactive workshops conducted throughout the year focused on practical applications of risk management principles. Participants engaged in scenario planning and real-time case studies, enhancing their skills in identifying and mitigating risks across various industries. This hands-on approach was especially beneficial, allowing attendees to collaborate and learn from one another, and to develop effective risk management frameworks that they could apply in their organizations.

## **Webinars: Expanding Accessibility**

Webinars offered a platform for those unable to attend in-person events to benefit from the wealth of knowledge shared by experts. These sessions covered a broad spectrum of topics including stress testing, risk culture, and digital transformation in risk management. The flexibility of webinars enabled professionals from all over the world to participate, fostering an inclusive environment for knowledge sharing and networking.

## **Thematic Focus on Sustainability and ESG**

A pronounced focus on sustainability and Environmental, Social, and Governance (ESG) factors emerged through various events. As organizations increasingly recognize the importance of responsible business practices, sessions centered on integrating ESG frameworks into risk management strategies were particularly impactful. Attendees learned how to assess and manage risks associated with climate change and social responsibilities, equipping them to lead their organizations toward sustainable futures.

## **Networking Opportunities**

The 2024 events also served as excellent networking platforms, bringing together professionals to exchange ideas and forge new partnerships. The collaboration between attendees from different sectors facilitated the sharing of best practices and innovative solutions, proving that risk management can benefit from a cross-disciplinary approach.

## **RiskPro's Participation in Key Events**

In 2024, RiskPro attended and hosted several significant events, enhancing our visibility and networking opportunities. Notably, we served as the Proud Gold Partner at the 28th Annual Conference 2024 - ISACA

Mumbai, and participated as the Exhibit Partner at the 8th Third Party Risk Management India Summit on 21-22 May 2024, in Mumbai. Additionally, we were the Associate Sponsor for the ISACA Chennai conference and held a Silver Partnership for the 5th Annual BFSI Operational Risk Management India Summit on 23-24 July 2024.

Our commitment to education and outreach included conducting 18 webinars throughout the year, covering topics such as:

- Segregation of Duties (SOD) - A Tool to Manage Risk
- ESG Reporting
- Anti-Money Laundering (AML)
- Integrating DAST into Your CI/CD Pipeline
- AI in Internal Audit

These webinars provided valuable insights into various aspects of risk management, ensuring that professionals remain informed and empowered in their roles.



## Recap of the Emerging Privacy and Security Risks Workshop

On April 24, 2024, professionals from various sectors gathered in Mumbai for the "Emerging Privacy and Security Risks" workshop organized by RiskPro. This event proved pivotal for those seeking to understand the rapidly changing landscape of privacy and security challenges in the digital age.

### Looking Ahead

As we set our sights on 2025, the insights gleaned from the 2024 conferences, webinars, and workshops underscore the importance of continual learning and adaptation in the field of risk management. RiskPro remains committed to providing high-quality learning experiences and will continue to explore emerging trends and challenges in the future.

Stay tuned for our upcoming events, as we aim to cultivate an even richer learning environment for professionals navigating the ever-evolving landscape of risk management.

### Objectives and Themes

The workshop aimed to equip attendees with knowledge about emerging privacy threats and security vulnerabilities that organizations face today. With the increasing reliance on technology, understanding how to navigate these risks is essential for

businesses to protect sensitive data and maintain compliance with regulations.

### Key Takeaways

- **Understanding Emerging Risks:** Sessions highlighted significant privacy concerns tied to advancements in technology, particularly the use of artificial intelligence and big data.
- **Interactive Learning:** Attendees engaged in exercises and discussions, fostering a practical understanding of risk assessment and management strategies.
- **Regulatory Frameworks:** Participants gained insights into current data protection regulations, emphasizing the importance of compliance.
- **Crisis Management Strategies:** Experts discussed how to prepare for data breaches





# Training and Learning - Riskpro Academy

-Anita Jagasia

Learning offers numerous benefits that enhance personal and professional growth. Gaining new knowledge increases confidence and adaptability especially in competitive corporate environments. In a professional setting, continuous learning boosts career opportunities, leading to higher salaries and job security. Online learning platforms have made skill and knowledge enhancement so much easier, accessible and affordable.

## Overview of Riskpro Academy

Keeping this in mind, Riskpro India has created the Riskpro Academy platform in 2021 to facilitate online learning for GRC professionals. Riskpro Academy is a specialized online learning platform focusing on risk management, compliance, and financial crimes. Over the past 4 years, we have more than 19,000 registrants on our platform enhancing their concepts through our online GRC courses!

The academy offers a range of free beginner courses, including overviews

on SOC Audits, ISO 27001, HIPAA, GDPR, Data Privacy, Anti-Bribery & Anti-Corruption, Anti-Money Laundering among many more topics to help learners grasp fundamental concepts.

## Our Top 5 Popular Courses

- **Environmental, Social and Governance (ESG) Compliance (For Beginners):** The course provides an overview on ESG, its criteria, importance of ESG, frameworks, ESG Reporting, ESG regulation worldwide and in India.
- **Overview of Anti-Money Laundering (For Beginners):** The course explains the concept of Money laundering, what is considered as an offence, terrorist financing and how to mitigate it using KYC and more.
- **Fraud Investigation & Internal Audit Overview:** The course explains What is Fraud, Types of Fraud, Why Do Frauds Happen, Fraud and the Law, Internal Auditing's Role in Fraud

Investigations, Roles and Responsibilities in Fraud Prevention/Detection, Fraud Risk Assessment and more.

- **Anti-Bribery & Anti-Corruption Overview (For Beginners):** This course provides an overview on Anti Bribery and Anti-Corruption. It explains about the standard ISO 37001, Do's and Don'ts. The course also explains the Prevention of Corruption [Amendment] At, 2018 and also gives the guidelines.

- **SSAE 18 (SOC Audits) Overview (For Beginners):** This course includes the Background of SSAE, SOC assessment process and parties involved, Third Party Engagements and their Risks and SSAE 18 and it's assessment types and reports.

### **Certified Global Compliance Specialist Course**

For professionals seeking advanced knowledge, Riskpro provides specialized paid certifications like the Certified Global Compliance Specialist (GCS). The GCS course is a combination of 9 courses providing a high level overview of topics like HIPAA, Anti-Money Laundering, Anti-Bribery & Anti-Corruption, SEBI Listing Obligations and Disclosure Requirements (LODR), Foreign Corrupt Practices Act (FCPA),

Prevention of Insider Trading, GDPR, Global Compliances and Building An Effective Compliance Framework. On completion of these 9 courses, participants need to take an online examination and will receive a certificate on successful completion of the course.

### **What's more?**

For learners who prefer audio based learning, Riskpro Academy also hosts audio recordings of all previously conducted Riskpro webinars on current topics such as IT compliance and data protection, enabling professionals to stay updated with evolving regulations. By combining comprehensive course offerings with self-paced learnings, Riskpro Academy serves as a valuable resource for individuals aiming to advance their careers in risk management and compliance.

For more details, you can visit [www.academy.riskpro.in](http://www.academy.riskpro.in) to browse various course categories as per your learning needs.



# HR Initiatives at Riskpro in 2024-25:

-Sonali Singh

- **Streamlined Organizational Structure**

A well-structured organizational framework has been a pivotal element in HR initiatives, focusing on enhancing efficiency and achieving business objectives. By emphasizing streamlined execution and delivery processes, HR has successfully improved its performance. This strategic approach ensures that HR operations are not only effective but also aligned with the company's culture and long-term goals.

**1.HR Metrics with KRAs and KPIs :** Incorporating Key Performance Indicators (KPIs) has played a crucial role in measuring the effectiveness of HR initiatives.

**2.Enhanced Leave Policy at Riskpro:** Riskpro's comprehensive leave policy aims to provide clear guidelines for employee leave entitlements, encashment, and the process for requesting and utilizing leave.

**3.Travel and Conveyance Policy:** Riskpro's Travel and Conveyance

Policy is designed to provide employees with clear guidance on reimbursement and travel-related expenses.

#### **4.Annual Employee Picnic Across India**

The Annual Employee Picnic brought together employees from various regions, strengthening team bonds and reinforcing the company culture. This event provided an excellent platform to celebrate achievements, with outstanding employees being recognized through awards and certificates. Thoughtful planning, including travel arrangements, engaging activities, and employee preferences, ensured a memorable and enriching experience for all Riskpro employees.

- **In 2025, Riskpro sets the following detailed breakdown key aspects of our progress and direct in Human Resource.**

#### **1.Launch Training and Development Programs:**

Employee training and development initiatives to enhance their skills, knowledge, and overall professional

growth. This includes providing access to various learning opportunities and hands-on training sessions. Riskpro helps its employees stay updated with industry trends, improve their performance, and prepare them for future challenges. Additionally, continuous development fosters a culture of learning, boosts employee satisfaction, and increases retention by demonstrating a commitment to their career advancement.

## 2.Ongoing Employee Engagement and Retention:

Strategies to enhance employee engagement and retention, including fostering a positive work culture. Encourage diversity and inclusion by cultivating an inclusive workplace. Prioritize employee well-being by introducing programs that support team work and mental health.

### **Employee Engagement at Riskpro**

At Riskpro, we prioritize a vibrant and connected work culture through regular employee engagement activities. From festive celebrations to team-building events, we create opportunities for our team to bond and unwind.

We celebrated Diwali in-office with traditional decor and joyful team i

nteractions. On Women's Day, we hosted fun games and engaging activities to honor the women in our team. Christmas brought festive cheer with a lively treasure hunt that encouraged teamwork and creativity. Regular team-building sessions further strengthen collaboration and create a positive work environment. At Riskpro, we believe that a happy team is a successful team.



---

# Our Leadership



**Manoj Jain**  
Founding Director

manoj.jain@riskpro.in  
9833767114



**Casper Abraham**  
Director

casper.abraham@riskpro.in  
9845061870



---

# Our Super Team



Rita Shewakramani  
EVP - Internal Audit  
and Risk Advisory



Vivek Dixit  
EVP - Risk and  
Governance



Laxmikant Gupta  
Principal



Ashok Agarwal  
EVP - IT Risk Advisory



Ritu Thakkar  
SVP  
IT Risk Advisory



Nitesh Shanbhag  
Senior Advisor - Business  
Transformation and  
Strategy

---

# Our Super Team



Niveditha Hampiholi  
SVP – IT Risk Advisory



Sucheta V. Upendra  
SVP – Information Security



Natarajan Mohan  
SVP – IT Risk Advisory



Raghavendra Mishra  
AVP  
Business Development



Vinaya Puneekar  
SVP – IT Risk Advisory



Ruchita  
AVP - HR and Recruitment



# Contact Details

**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.

**For regular updates follow us at**



[info@riskpro.in](mailto:info@riskpro.in)



[www.riskpro.in](http://www.riskpro.in)





# **Riskpro Magazine**

**2025**

# **Thank You**

---