AI- and data-powered integrated risk management

Consider a few real-life scenarios that illustrate the multidimensional nature of risks business face today:

- The accountant of a chemical manufacturing company siphoned off INR 32 crore over a period of eight years by presenting tax payment cheques to the management for signing and later adding his own account number on them after they were signed. Subsequently, the balance in advanced tax payment was transferred to the cost of production account (meant for system-generated postings).
- A large e-commerce company in India is facing a security issue wherein its order data is being leaked/hacked post which customers receive fake emails and SMSs containing links to update their details. Subsequently, customers' accounts are taken over by hackers, who place fraudulent cash on delivery (CoD) orders and use the funds in their wallet.
- A bank's retail lending department recently discovered that its retail loan portfolio was showing increasing defaults. Investigations revealed that the salary credits shown by a customer in their bank statement were not authentic. Deposits were created for the same amount every month with the description of a large employer/company, following which there were withdrawals in multiple instalments.
- Multiple retail and credit card companies have been facing regular instances of chargeback/digital payment frauds whereby some customers buy low-value items through their e-wallet and immediately raise a fraudulent debit incident with the wallet company to get the amount credited back into their account.
- In 2020, a card and payment transaction processing company filed for insolvency after unearthing inflated revenue and cashflows worth EUR 1.9 billion.
- In FY22, the Reserve Bank of India (RBI) levied penalties worth INR 65.32 crore in 189 cases across various financial institutions for non-compliance with guidelines on matters related to KYC , exposures norms, Unique Customer Identification Code (UCIC) and advances to key managerial persons (KMPs), directors, etc.

It is becoming increasing difficult for businesses to keep pace with the growing number of risks using conventional mechanisms such as audits, investigations, controls self-assessments and post-mortem reviews.

As per Association of Certified Fraud Examiners (ACFE) estimates, businesses incur a loss of about USD 4.7 trillion annually on account of frauds and governance issues. Another industry estimate suggests that businesses face leakages to the tune of 1–5% of their year-on-year revenue on account of control weaknesses. At the same time, the global cost of cybercrime was USD 6 trillion in 2021.

Therefore, businesses cannot afford to adopt a reactive approach to such risks. Proactive mechanisms have to be adopted in order to minimise the impact on revenue, reputation and growth. This can be enabled only by a multidimensional risk monitoring mechanism supported by data and artificial intelligence (AI).

Boards and top management are also looking at organisation-wide risk views that allow them to understand the criticality as well as the impact of various risks on their business, and thus prioritise the most critical issues.

This has given rise to the concept of data-driven integrated risk management, which involves setting up an integrated mechanism to monitor multi-dimensional risks that a business faces on a day-to-day basis.

Building a data-driven integrated risk management system

1 **Monitoring framework**
Define risk monitoring framework, reporting structure, roles and responsibilities.

2 **Assessing risks**
Identify risks that require ongoing monitoring.

3 **Map risks to KRIs**
Break up risks into multiple KRIs and risk measurement attributes.

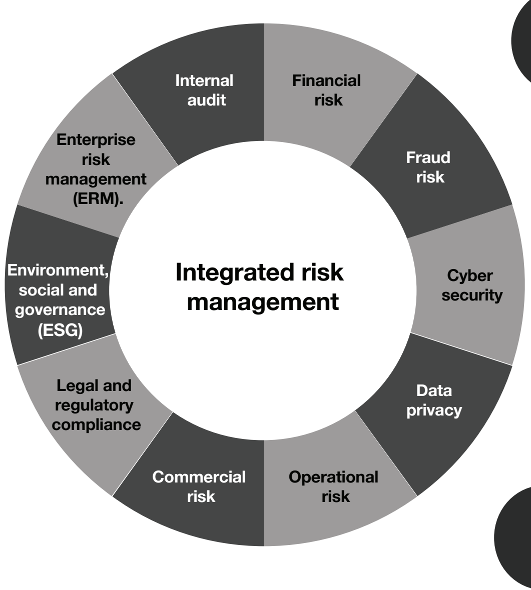
4 **Map KRIs into analytics**
Map KRIs to analytical statements where possible.

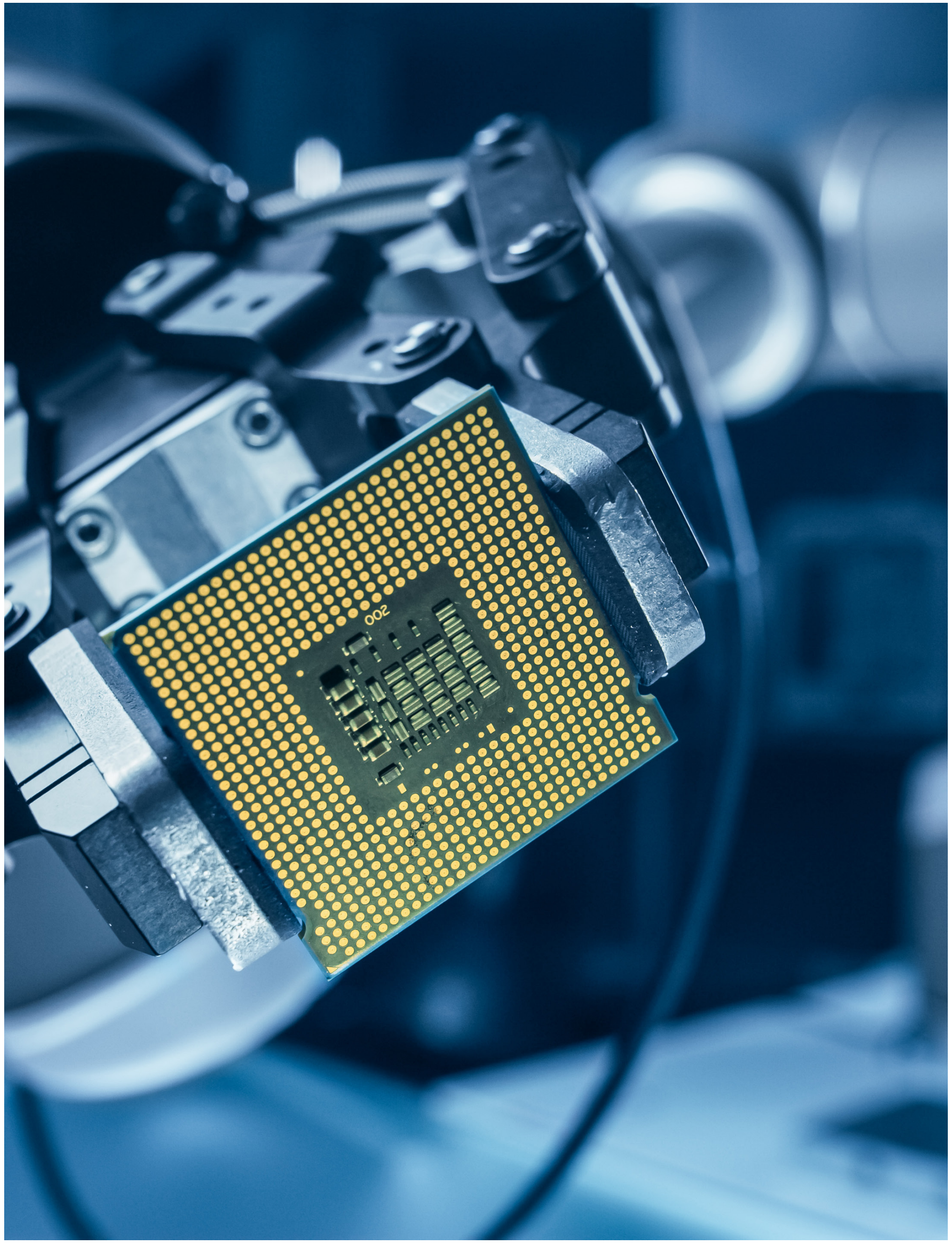
5 **Sources and data mapping**
Map risk measurement attributes and analytics to data and information sources.

6 **Building the platform**
Design and implement solution to allow data integration from various sources, processing, reporting and action.

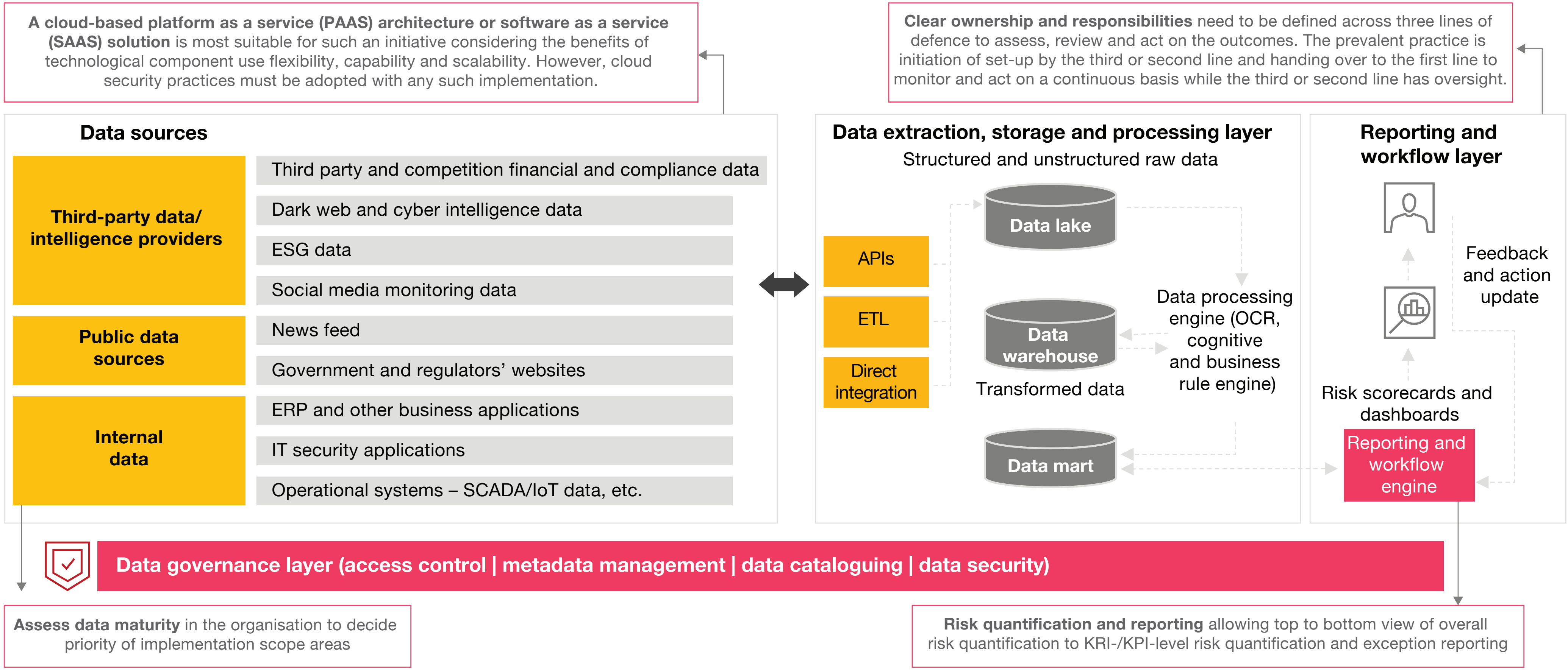
7 **Data governance**
Mechanism to ensure that the platform protects, manages and uses the data to provide desired outcomes.

8 **Risk quantification**
Reporting risk score and impact along with status of actions for prioritisation of efforts for improvement.


Integrated risk management
Internal audit
Financial risk
Fraud risk
Cyber security
Data privacy
Operational risk
Commercial risk
Legal and regulatory compliance
Environment, social and governance (ESG)
Enterprise risk management (ERM).



Indicative architecture for an integrated risk management system



A cloud-based platform as a service (PAAS) architecture or software as a service (SAAS) solution is most suitable for such an initiative considering the benefits of technological component use flexibility, capability and scalability. However, cloud security practices must be adopted with any such implementation.

Clear ownership and responsibilities need to be defined across three lines of defence to assess, review and act on the outcomes. The prevalent practice is initiation of set-up by the third or second line and handing over to the first line to monitor and act on a continuous basis while the third or second line has oversight.

Data sources

Third-party data/ intelligence providers

- Third party and competition financial and compliance data
- Dark web and cyber intelligence data
- ESG data
- Social media monitoring data

Public data sources

- News feed
- Government and regulators' websites

Internal data

- ERP and other business applications
- IT security applications
- Operational systems – SCADA/IoT data, etc.

Data extraction, storage and processing layer

Structured and unstructured raw data

APIs

ETL

Direct integration

Data lake

Data warehouse

Transformed data

Data mart

Data processing engine (OCR, cognitive and business rule engine)

Reporting and workflow layer

Feedback and action update

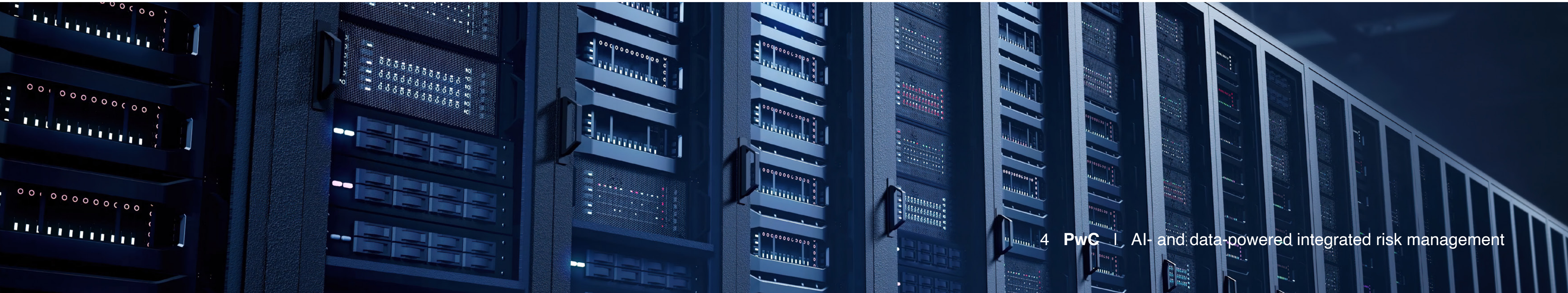
Risk scorecards and dashboards

Reporting and workflow engine

Data governance layer (access control | metadata management | data cataloguing | data security)

Assess data maturity in the organisation to decide priority of implementation scope areas

Risk quantification and reporting allowing top to bottom view of overall risk quantification to KRI-/KPI-level risk quantification and exception reporting



Use of AI in the integrated risk management process

Dimensions of integrated risk management	Key risk dimensions	Data	Role of AI/ML	Examples of AI tools and vendors
Financial risks	Inflated/deflated valuation, recording and reporting of assets, liabilities, income, expenses, cash flows, disclosures, etc.	**Internal:** Financial statements, trial balance, general ledger (GL) transactions, financial market transactions, access rights and privileges **External:** Industry benchmarking and financial information from sources such as, MCA SaveRisk InstaFinancials and other global financial benchmarking platforms	• Detection of GL transactions and balances outlier for various dimensions of abnormal values and time, GL code, user ID wise manipulative entries • Automated valuations and model validations	• GL.ai • Provenir • Fidelity National Information Services (FIS)
Operational risk	Revenue/cost leakages, operational efficiencies/ productivity issues, employee conduct, negative reviews and feedback from customer, physical security and safety events (strike, accidents, attack, disasters, etc.)	**Internal:** Business process transaction data, loss events, loss data, customer complaints data, employee grievances and feedback survey data, security recordings and logs, internet of things (IoT) data **External:** External loss events, industry benchmark on operational performance, natural calamity/disaster prediction data, news and social media listening data	• Detect abnormal patterns in transactions such as out of the order/abnormal purchase/sales/ production/quality event or transaction • Predict operational failures/downtimes/risk event • Identify operational efficiency improvement opportunities	• Celonis • Fusion • Mentionlytics
Cyber security and data privacy	Financial and operating system downtime/failures, funds misappropriation, sensitive data leakage and regulatory implications	**Internal:** IT assets and network inventory data, threat alerts and security breach event logs, endpoint and user behaviour data **External:** Dark web intelligence data, social media data	• Cyber risk quantification • Faster detection of anomalies in user and transaction behaviour • Security incident/vulnerability prediction • Prioritised alerts to optimise remediation efforts	• Flashpoint.io • Fair Isaac Corporation (FICO) WhoisXML API • Bitsight Technologies
Supply chain and third-party risk	Supply chain disruption such as material procurement delays, operational breakdown, data security issues, legal, compliance and reputational risk	**Internal:** Supplier/vendor masters, supplier/vendor transactions and performance data, contractor staff and access data, etc. **External:** Third-party financial health information, compliance data, litigation data, public domain negative event data, fourth party concentration risk, background verification data, vendor ESG score	• Predicting supply chain disruption • Automated vendor due diligence • Detecting related parties, suspicious patterns or anomalies	• Blue Yonder • Signal Media
Fraud risk	Company assets/funds misappropriation/theft, financial crime, digital payment fraud, social engineering threat intelligence, bribery, corruption, sanctioned/ politically exposed person (PEP) entity dealing risk, fake news/media, counterfeit products, etc.	**Internal:** Business transaction data, business documents, user ID, geolocation, IP address, customer, employee and vendor master data, etc. **External:** Customer/individual identity data, corporate entity identity data, PEP data, sanctioned entity data	• Fraud risk prediction such as customer/vendor favouritism • Real-time fraud detection for payment and AML transaction • Identify theft/misuse identification • Document tampering identification (e.g. fraudulent invoices/background check documents/claims documents)	• Cyabra • SymphonyAI • VineSight • KonaAI • Gradiant • Equifax

Dimensions of integrated risk management	Key risk dimensions	Data	Role of AI /ML	Examples of AI tools and vendors
Regulatory and compliance	Regulatory non-compliance and penal consequences such as anti-money laundering (AML) violations, KYC failures, consumer protection violations, surveillance, sanctions and transactions risk; fiscal, labour, and environment health and safety (EHS) non-compliances, etc.	**Internal:** Regulatory and statutory compliance checklists, compliance documents, compliance reporting related business data **External:** Regulatory/compliance requirement library, regulatory and government websites for circulars, notifications and updates, watchlist data, etc.	• Automation of regulatory requirement tracking interpretation and summarisation • Document review for compliance assessment • Risk data mart for regulatory and risk reporting	• Cube • Actio
ESG	ESG reporting inaccuracies, compliance and policy breaches on ESG norms, rejections of proposals and products from investors and customers, etc.	**Internal:** Energy/water consumption, waste output/treatment, health and safety KPIs, gender ratio, tax paid, employee retention rate **External:** ESG scores, green gas emissions, air quality index (AQI), waste management, human rights, labour practice, gender ratio, management quality	• Benchmarking with peers on ESG KPIs • Automated ESG due diligence • Insights by processing corporate communications, investor transcripts, etc.	• Ecovadis • Refinitiv • Novisto
Contractual and commercial risk	Legal exposure beyond approved appetite, lawsuits and disputes with contractual parties, breach or ignorance of commercial terms causing commercial loss, etc.	**Internal:** Contracts/agreements, customer/vendor/service provider business transaction data, contract risk management policy External: Industry standards for contractual clauses/agreement templates	• Assessment of legal exposure and liability risk in contracts, extracting insights • Contractual terms and conditions abstraction, interpretation and summarisation	• Harvey AI • Diligen
Internal audit	Insufficient coverage of audits, statutory audit qualification, ineffective audit issue management causing repeat control failures, leakages and governance issues	**Internal:** Internal audit universe, financial statements, internal audit reports, issue closure tracking information **External:** Industry risks insights	• Unstructured data analytics such as text and image analytics in document review • Automated audit processes by intelligent automation	• Workiva • HighBond
ERM	Business growth/sustenance challenges, reputational risk, business disruption risks	**Internal:** Risk appetite metrics, strategic/enterprise risk library, key risk indicators (KRIs), mitigation plans, financial, operational and security data **External:** Macroeconomic data, social media, blogs, news, competitor information, industry benchmarks, application and security performance standards, etc.	• Enterprise-level early warning system/risk measurement and quantification linked to KRI assessment based on external data/intelligence	

However, establishing the above mechanism is not the end but a start. Like any business that needs to stay up to date with the changing environment, consumer demand and competitive landscape, a risk management system also needs continuous enhancement and refinement in the face of a changing risk landscape, technology and information availability.

Groundwork for implementation

Implementing an integrated risk management system can be a major change or transformation initiative for any organisation. Hence, it is important to do the required groundwork to prepare oneself effectively . This groundwork involves the following key aspects:

a. **Senior management buy-in:** A large transformation like this is most successful when it has the support of the board and top management. To obtain this support, the vision has to be clearly articulated; requirements, clearly assessed; benefits, clearly understood and explained; and a path to implementation, clearly laid out.

b. **Measuring cost of risk to the business:** Measure (1) man-hours cost of monitoring controls and compliance in a year and (2) financial cost of failures of controls (financial leakages, revenue loss, etc.), delays/non-compliance with statutory/regulatory requirements, fraud and cyber incidents in the last 12 months. Once an organisation has measured the cost, it has to identify areas where integrated risk management could reduce the cost to the company and present a return on investment (RoI) analysis.

c. **Functional and technical know-how:** Organisations need to bring on board the right team/people who understand the industry, respective domains of risk (cyber/IT/fraud/internal audit/regulatory compliance/ESG/supply chain, etc.), as well as those with technical competencies around technology, data, security and application development. Given the long road to learning and implementation in an in-house development model, adopting an established platform or combining internal capabilities with an external platform should be the preferred mode.

Implementing an integrated risk management framework may challenge organisations and initiative owners to think big and make bold moves rather than taking small steps over a long period of time. However, considering the pace of technological advancements the world is witnessing, organisations that think ahead of the curve instead of following or ignoring the current trends will be more prepared to face the future with confidence.

ChatBot
AI
AI
OK I can answer your question in several ways:
1) The neural network that provides you with the math should be constantly monitored
2) Adjustments should be made to any feedback loop providing corrections
3) Statistical data may need to be updated
4) Analysis of that statistical data has to be checked / fact c
5) Inputs have to be reco understood

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.
Please see www.pwc.com/structure for further details.

Contact us

Shreyans Dudheriya
Partner, Risk Consulting – Risk Assurance Services
PwC India
shreyans.dudheriya@pwc.com
+91 97170 07225

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

KS/August 2023 - M&C 30789