Risk quantification is at a critical crossroads.

Traditional risk quantification

Business risk exposure

Stifling innovation

Difficult to understand

Identifying potential risks

- Heavily manual review of processes
- Dependent on self-reporting or weak triggers

Assessing risk

- Ad-hoc, reactive, not standardized
- Criteria and standards shifted depending on circumstances
- Assessment results and other data not centralized and reusable

Measuring risk

- Fixing a problem stems from an individual assessment
- Takes a control view and averages risk scores
- Risk modeling is limited to the system level

Managing and monitoring risk

- Disparate sources of assessment that do not build on each other
- Triggers based on control importance or uninformative key risk indicators (KRIs)
- Scope review is based on independent risk assessment

Risk reporting

- Inherent and residual risk are plotted on heat map
- Difficult to compare operation and technology risk events
- Reports are based on materiality of incident

Forward-looking risk quantification

Managing tech risk

Unleashing the power of technology

Driving business value

Identifying potential risks

- Systematic identification through modeling environment
- Proactive assessment of emerging risks and threats

Assessing risk

- Expresses risk in business/financial terms
- Rationalize, prioritize, and enhance risk mitigation activities
- Identified sources that feed assessment of what can be automated

Measuring risk

- Prioritizes across findings based on relative impact. Makes decisions at a finer level of detail
- Uses all available tech risk data and applies accepted statistical principles to express risk
- Accounts for the relationship between control, systems, threats, and business impact

Managing and monitoring risk

- Understands the cost of the control and right investment within risk tolerance
- Consolidates all forms of assessment to determine aggregate management effectiveness of controls
- Monitors metrics that inform the overall management effectiveness of controls or impact on risk

Risk reporting

- Only residual risk to the organization at varying level of confidence/probability
- Operational and technology risk events denominated in financial loss
- Evolving view of what constitutes materiality

Learn more:
advisory.kpmg.us/articles/2020/tech-risk-intelligence.html

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

KPMG