Integrated Risk Management

Sustainable Strategic Decision Making

The requirements of digital businesses are rapidly changing, meaning governance, risk and compliance (GRC) activities must evolve to encompass an integrated approach to risk management. Increasingly, organizations are looking for tools that synthesize, integrate and visualize all forms of data to facilitate enterprise level risk management decision making.

Historically, both vertical and horizontal based risk were addressed by isolated disparate teams with little to no data synthesis. Advancing technology and more complex regulatory requirements are, however, forcing C-suite executives to review this practice and integrate risk analysis into their decision making.

Breaking down siloes to gain control and visibility over one area of risk will in turn improve decision-making and business intelligence across other parts of the organization. Ultimately, integrated risk management makes it possible to understand the wider business implications and ask more strategic questions.

Definitions

Governance – The act of controlling, and evaluating an entity, process or resource.

Risk Management – The act of managing processes and resources to address risk while pursuing reward.

Compliance – The state of being able to prove fulfilment of a requirement, obligation, commitment, policy or value.

Integrated Risk Management (IRM) – A set of practices and processes that improve decision making and performance through an integrated view of how an organization manages its unique set of risks.

Types of Risk Areas Encompassed Within IRM

Although not an exhaustive list of risk areas, the following give a flavor of what could be included:

Corporate Compliance Management – Increasing complexity of compliance with new regulations such as GDPR.

IT Risk Management – The disruption of traditional risk models by IoT, machine learning and big data. New and emerging technologies will require a rethink on the sources of IT Risk.

Business Continuity Management - The ability to identify, respond to, and recover from business disruptions is critical to the success of the modern digital organization.

Third Party Risk – The reliance on complex vendor supply chains and geographical location issues.

Corporate Compliance Management

Corporate compliance management is undertaken by policies and guidelines. Adherence to internal and external governance ensures the integrity of the organization.

Regulatory non-compliance incurs large fines and an accompanying reputational risk. Non-compliant staff face official warnings or in severe cases could face dismissal for continued non-compliance.

Organizations are instilling a risk aware culture and complementing this with learning and development programmes, ensuring staff members are compliant and aware of their responsibilities in mitigating potential risk.

Dashboard reporting to the CRO on the level of staff regulatory compliance ensures that effective communication is in place to protect the integrity of the organization.