Camms.Risk

Whitepaper

Eight red flags that indicate you need a better risk management approach

Camms.

No matter who you are or where you work, risk management is relevent, even more so in today's climate.

Around the globe, businesses are experiencing change like never before. At the same time, new regulatory requirements are emerging to govern privacy, data and to standardize common business practices.

As businesses evolve and adapt to thrive in a digital future, it is inevitable new areas of risks will emerge.

Organizations everywhere face the challenge of pursuing fresh opportunities while simultaneously protecting themselves against damage. Damage to their reputation, customer and partner relationships, data, employees, financial position and more. Clearly, risk strategies need to keep pace with our rapidly evolving world.

Implementing a governance, risk and compliance (GRC) framework is the first step to building a truly effective risk management approach.

Beyond that first step, utilizing smart software in conjunction with the GRC framework enables an integrated, flexible risk-management structure able to power a business with fast, actionable insights.

Where to begin?

Start with addressing a few basic questions:

1. What can go wrong on the path to our organization achieving its strategic objectives?
2. What do we have in place to stop something going wrong?
3. How effective are those controls?
4. How will we know something has gone wrong?
5. Who needs to know something has gone wrong?
6. What more should we be doing?

Exploring answers to these questions is a good test of the effectiveness of an organization's risk management strategy.

Eight red flags that indicate you need a better risk management approach

Some organizations treat risk management as a “tick the box it’s done” exercise. This falls well short of an effective risk management approach. Signals that indicate risk management could be improved, include:

1 In-house tools and spreadsheets.

In-house tools are typically built by IT departments. This poses several challenges to risk management. First, employee retention becomes vital to the continuity of the platform. If the employee who built the proprietary risk management system walks out the door, so does the intellectual property to run, maintain and upgrade the system. Second, technology and regulations evolve far more rapidly than most IT departments can keep pace against. Third, most IT departments are resource constrained by having to support all IT demands across an organization. Fourth, manual management of risk in spreadsheets means slower, less accurate, siloed capturing of risk and hazards resulting in less effective mitigation actions and reporting.

2 Pure compliance focus.

Some organizations see risk management solely as a box ticking exercise necessary to meet an internal or external requirement. Successful organisations place positive value on risk management at all levels. In these organizations, risk management is not seen as a tedious, compliance process. Instead, it is seen as a core strategic and operational process to better identify and manage threat and opportunity based risk.

3 Risk management is an isolated discipline.

Risk management functions operating in silos or as back-office functions can quickly become disconnected from business reality. Increasingly there’s demand for risk management insights to be integrated into Board and performance reporting. Why? Boards, executives and managers need regular visibility and performance reporting on risk to guide decision making and successfully achieve organizational objectives.

4 Strategic and operational risks are missing or poorly defined.

The most successful organizations adopt a regular process to identify, assess, rank and treat strategic and operational risks across their business. Strategic risks are driven externally or elevated in importance from an internal operating environment. Operational risks typically include both enterprise level and service level risks. Poor processes to regularly identify, assess and review risks from either external or internal sources signals the need for an improved risk management strategy or better implementation of an existing one.

5 No controls identified and assessed for risks.

Organizations who manage risk well have clear internal control frameworks used to identify, assess and improve risk controls. If this is missing, it can lead to a poor understanding of residual or current risk status as well as increasing exposure to those risk events.

6 De-centralized visibility.

Managers and executives need fast, accurate visibility into risks across strategic, operational and project landscapes. Often what appears to be an isolated risk will impact other areas of the business. Stakeholders have no context for the implications of risks across the entire business without a single source of visibility. Gathering insights from multiple sources and synthesizing the data consumes valuable time and resources which could be directed to managing high impact risks in the business.

7 No dedicated resources.

An absence of dedicated resources can signal a lack of focus, investment, awareness and commitment from senior leadership that risk management is a strategic priority for the organization. Organizations don't necessarily need a Chief Risk Officer, but they do need identified resources to drive effective risk management.

8 Lack of Executive sponsorship.

It is all too common for executives to avoid making decisions on risk management because there's no compelling event to drive an investment decision. Until it is too late. As for any enterprise-wide deployment, proactive executive commitment is needed to drive investment in, and focus on, risk.

Benefits of effective risk management

The benefits of effective risk management are powerful for every business and include:

— Empowering stakeholders to constructively assess and plan for and respond to risk events by having the right information, quickly available.

— Strengthening informed decision-making by offering leaders a clear, consolidated view of governance, risk and compliance and risk exposure across an entire business.

— Improving audit-ability and risk traceability through more efficient and effective data recording.

— Integrating risk management into all business management processes so incidents don't become major business issues.

— Freeing up employee time to focus more on proactive risk and compliance strategies and less on reactive fire fighting.

— Gaining valuable insights to enable education and training of a more risk-aware workforce.

— Having insight to risk information anywhere, anytime via mobile technology.

Getting more out of your risk management

There are some compelling reasons to partner with an industry recognized risk management provider like Camms:

— Visibility: understand what is happening across strategic, operational and project risk landscapes through simple, centralized dashboards

— Audit-ability: capture data effectively from multiple systems to power fast, accurate auditing of risk and hazard factors

— Remediation and response: develop control frameworks capable of responding effectively, rapidly and comprehensively to risk

— Reporting: provide Boards, executives and managers with the information they need, quickly and accurately, to support more informed decisions

Working with Camms allows businesses to align their risk management approach with industry leading practices and ISO 31000 requirements.

Camms. | Camms.Risk

United Kingdom
+44 (0) 161 711 0564

North America
+1 (212) 401 6905

Asia/Australia/New Zealand
+61 (0)8 8212 5188

sales@cammsgroup.com

For more information

VISIT WEBSITE

REQUEST DEMO