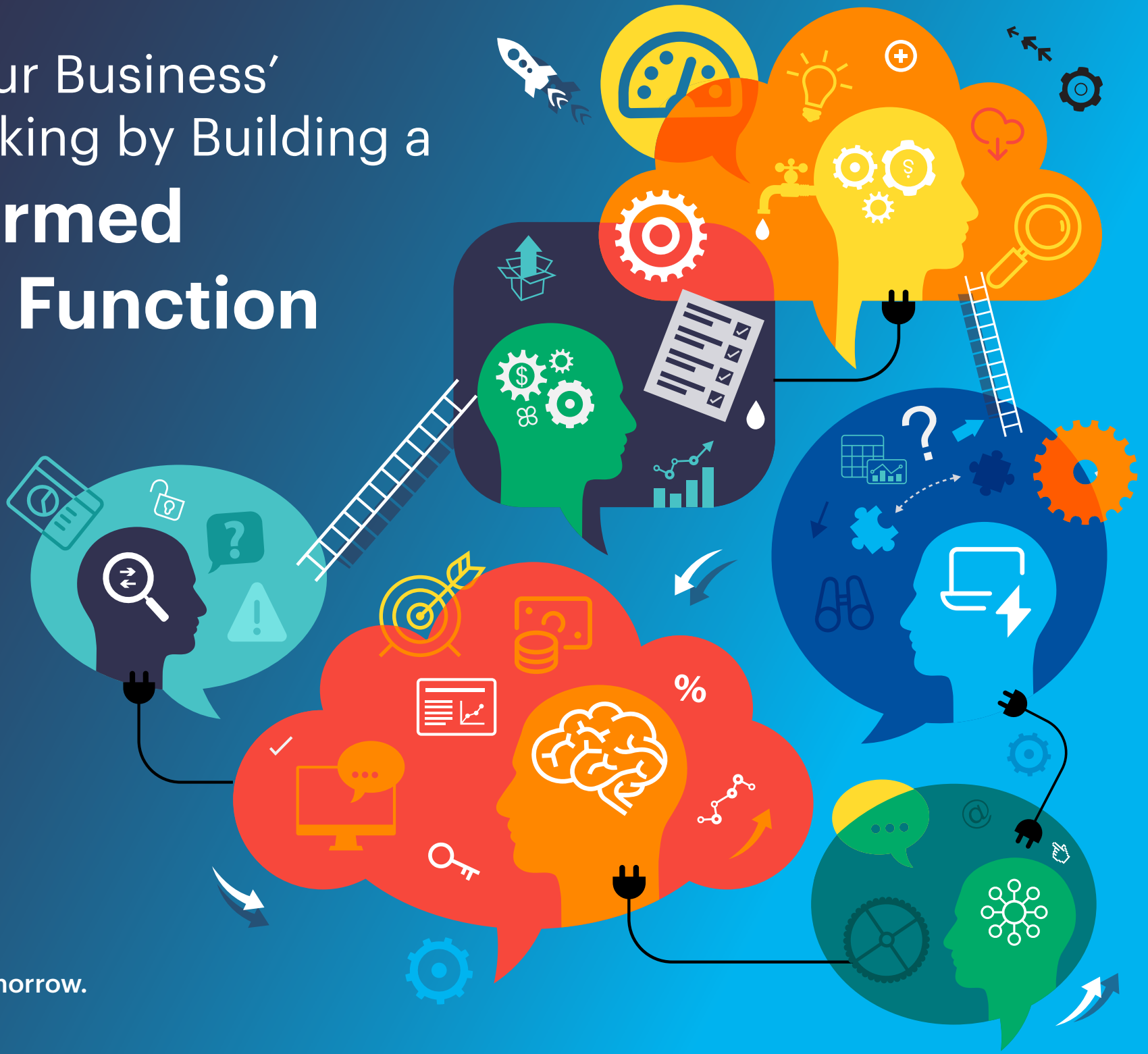
Maturing Your Business' Decision-Making by Building a

Risk-Informed Planning Function



Camms.

Software to Change Tomorrow.

Intro

Risk is omnipresent in businesses of all sizes – from operational risk and emerging risk to regulatory risk and financial risk. They are constantly exposed to these uncertainties that threaten their ability to generate a profit because risk is inherent to operations. Paradoxically, businesses must embrace risk because risk-taking is fundamental to achieving economic reward and generating opportunities that lead to evolution.

To strike a balance between risk and reward, senior decision-makers must recognize which risks have the greatest potential to impact the business and understand how to manage them to enhance performance, drive value creation and ensure sustainability – bringing proactive risk management into sharp focus.

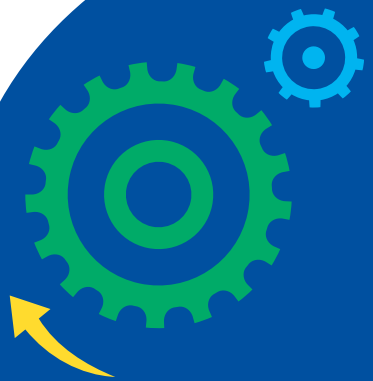
The adage 'prevention is better than the cure' rings true in the context of risk management. Businesses that adopt a reactive view of risk are hamstrung by a response-based approach that's dependent on incident evaluation and audit-based findings after an incident has occurred – restricting their ability to stop it from happening again.

Rather than crossing their fingers and hoping the risk will go away, they should empower themselves to react proactively by anchoring risk management into existing strategic planning processes. This will engender a culture of actionable risk-informed business decision-making from the top down that provides the foresight to prevent – or at least mitigate – risk.

Traditionally, there has been a disconnect between enterprise risk management (ERM) and strategic planning – the modus operandi of most businesses. Consequently, ERM programs typically lack the strategic foundations from which they can build organizational value by informing business decision-making and ensuring resources are allocated to risks.

This has resulted in a slow up-take of risk and strategy integration across sectors, which can be attributed to several factors, including:

- The adoption of simplistic or complex risk management models.
- Considering ERM as a compliance activity only, rather than an integral part of strategic and operational planning.
- A lack of understanding of how risk management, strategy development and execution should integrate.
- A lack of clarity about the organization's risk appetite, which can limit the development of opportunities or expose the organization to intolerable levels of risk.
- A lack of adoption by the board and senior executives, who fail to understand the value drivers of the organization, the risks associated with them and how to best manage those risks.



By overcoming these challenges and conflating risk management with the strategy, the ERM becomes aligned with the organization's strategic goals and objectives. From this new vantage point, ERM can be leveraged to help "run the business", rather than focusing on operational risks and protecting the enterprise – and the benefits are compelling: more explicit integration in business decision-making, increased focus on strategic and external risks, and an enhanced ability to use risk information to adjust business strategy.

How to Build a Risk-Informed Planning Function

The process of enhancing the business strategy from a risk perspective won't happen overnight – it must be underpinned by a willingness to understand the internal and external risk environment. From understanding the different types of risk they might face and how to manage them, to assessing their current stance on the risk maturity model, businesses must explore their risk exposure and capability before integrating it with planning and management routines.

Understanding Risk Exposure

The importance of aligning ERM with strategy must be a board priority. Boards that recognize the value of coupling strategic oversight with the methods and processes used to manage risks, can enhance business performance. A crucial element of this top-down approach to maturing risk management is understanding the types of risks the business will face and defining its risk appetite.

There are three key categories of risks, each requiring a different management approach that will benefit the business:

Upside Risks:

These present opportunities to enable the business strategy and achieve performance management objectives. Examples include product or service innovation and market expansion.

Outside Risks:

These arise from events outside of the organization's control – and can present negative results and/or positive benefits. Businesses can't influence the chance of these events occurring, but they can be prepared and mitigate the cost of impact. Examples include competition, legislation and natural disasters.

Downside Risks:

These risks occur within the organization and present only negative impacts. Therefore, they are controllable and should be prevented or avoided. Examples include cybersecurity, fraud and regulatory noncompliance.

Once the board understands the different types of risk, it will better understand how to manage them. For example, outside risks must be identified and mitigated through scenario analysis and stress testing to determine if the organization has the resources to absorb the full impact of these external events; whereas downside risks require proactive prevention controls and structured monitoring of the threat level to prevent them.

Understanding Current Risk Capability

The process of enhancing the business strategy from a risk perspective won't happen overnight – it must be underpinned by a willingness to understand the internal and external risk environment. From understanding the different types of risk they might face and how to manage them, to assessing their current stance on the risk maturity model, businesses must explore their risk exposure and capability before integrating it with planning and management routines.

A risk maturity model outlines key indicators and activities that comprise a sustainable, repeatable and mature ERM. This risk maturity self-assessment allows businesses to benchmark how inline their current risk management practices are with these risk attributes – such as:

Adoption of ERM-based process:
Measures a business's risk culture, which considers the degree of board or senior executive support for ERM.

ERM process management:
Measures the extent to which the business has adopted an ERM methodology throughout its culture and business decisions.

Risk appetite management:
Evaluates the level of awareness around risk opportunity, accountability for risk, defining risk tolerances, and the business's ability to close the gap between potential and actual risk.

Uncovering risks:
Measures the quality and coverage of a business's risk assessments by examining the method of collecting risk information, the risk assessment process and whether trends and correlations can be uncovered from the risk information.

Performance management:
Determines the extent to which a business delivers its visions and strategy, by evaluating its ability to plan, communicate and measure business goals using a risk-based process.

Business resiliency and sustainability:
Evaluates the extent to which sustainability activities such as business continuity and operational planning are approached with a risk-based methodology.

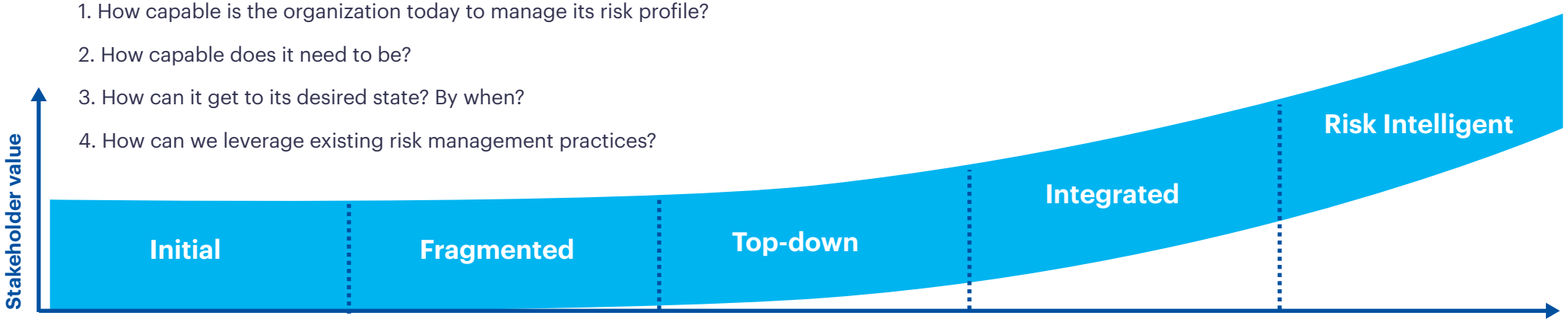
The goal is to move up the risk model and achieve strategic risk intelligence – as outlined by the Deloitte risk maturity model:

Risk Maturity Model

Understanding your risk capability - current and desired state

The goal is to move up the maturity model

1. How capable is the organization today to manage its risk profile?
2. How capable does it need to be?
3. How can it get to its desired state? By when?
4. How can we leverage existing risk management practices?



Stages of risk management maturity

- Ad hoc/chaotic
- Depends primarily on individual heroics, capabilities, and verbal wisdom

- Risk defined differently at different levels of the organization
- Risk managed in silos, and risk interactions identifired in limited manner

- Common risk assessment, program statement, policy
- Enterprise-wide integrated risk assessments
- Communication of top strategic risks to the board
- Executive/streering committee
- Knowledge sharing across risk functions
- Dedicated team to manage risk
- Awareness activities

- Coordinated risk management activities across silos
- Risk appetite fully defined
- Enterprise-wide risk monitoring, measuring, and reporting
- Technology-enabled processes
- Contingency plans and escalation procedures
- Risk management training

- Risk discussion embedded in strategic planning, capital allocation, product development, etc.
- Risk sensing and early warning risk indicators used
- Linkage to performance measures and incentives
- Risk modeling/scenarios
- Industry benchmarking used regularly

Source: Risk Intelligent Governance: Lessons From State-of-the-art Board Practices

A risk intelligent culture comprises the following characteristics:

- Risk accountabilities and responsibilities are understood and clearly defined.
- Appropriate policies and practices are implemented, including formal processes to communicate, escalate, and report risks.
- Employees are encouraged to challenge the organization.
- An engaging code of conduct that promotes the values and beliefs of the business.
- Risk management is supported by education and awareness, providing employees with appropriate skill sets, knowledge and other risk competencies.
- Risk considerations are incorporated into performance evaluations, and an established incentive structure promotes and rewards risk intelligent behavior and decisions.

By embracing this common risk management approach businesses can uncover dependencies and break down silos, leading to a more comprehensive ERM program that can be harnessed – and integrated – to create a risk-informed planning function.

Integrating Risk into Business Planning and Management Routines

Armed with an in-depth understanding of risk exposure and current risk capability, the integration of ERM into existing business planning and management routines can begin in earnest. The following steps provide the building blocks to achieve this:

Define the business strategy and objectives: This should be conducted and communicated by the board of directors – and must be as specific and as quantifiable as possible.

Establish key performance indicators (KPIs): These reactive indicators help a business to measure forthcoming results. Whether they are met or missed, KPIs will provide a roadmap for progress in the future by measuring historical performance.

Identify risks that can drive variability in performance: These are the unknowns that will determine results in the future – such as customer demand.

Establish key risk indicators (KRIs) and tolerance levels for critical risks: These proactive, forward-looking lead indicators are the opposite of KPIs because they are used to anticipate risk events that may occur in the future – and should be communicated from the top-down.

Provide integrated reporting and monitoring: Businesses must monitor KPI driven results and KRIs continuously to mitigate risks or leverage unexpected opportunities when they arise.

How Key Risk Indicators (KRIs) Can Add Value

KRIs can be defined as:

"critical predictors of unfavourable events that can adversely impact organizations. They monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises and mitigate them in time."

KRIs aren't concerned with monitoring every single risk the business is exposed to; they focus on the most critical indicators for managing the highest (key) risks – which vary from business to business in line with their objectives and priorities. What is considered a key risk for one business may not be important to another, or what was a key risk for a business last year may not be a key risk this year.

These indicators or metrics are used to measure risks that the business is exposed to – a kind of early warning system, like an alarm, that's triggered when risk exposure exceeds tolerable levels.

In this way, effective KRIs play a pivotal role in ERM by providing a foundation for monitoring and predicting potential high-risk areas and taking prompt action to prevent or mitigate their impact –

Enabling businesses to:

- Identify current risk exposure and emerging risk trends.
- Highlight control weaknesses and allow for the strengthening of poor controls.
- Facilitate the risk reporting and escalation process.
- Implement operational risk management that adds value.

Effective KRIs should be:

- Quantifiable – metrics should be measurable.
- Predictable – provide early warning signals.
- Comparable – track over a period to highlight trends.
- Informational – measure the status of risk and control.

Examples include:

- Financial KRIs: economic downturn and regulatory changes.
- People KPIs: high staff turnover and low staff satisfaction.
- Operational KPIs: system failure and IT security breach.

KRIs must be linked to the business's strategic priorities. Having defined its goals, the business can identify the key risks related to each goal and design KRIs that track those risks and act as an early warning system – flagging up when the business is at risk of not achieving its goals. Once in place, they must be monitored and tracked regularly – with the frequency dependent on the specific KRI.

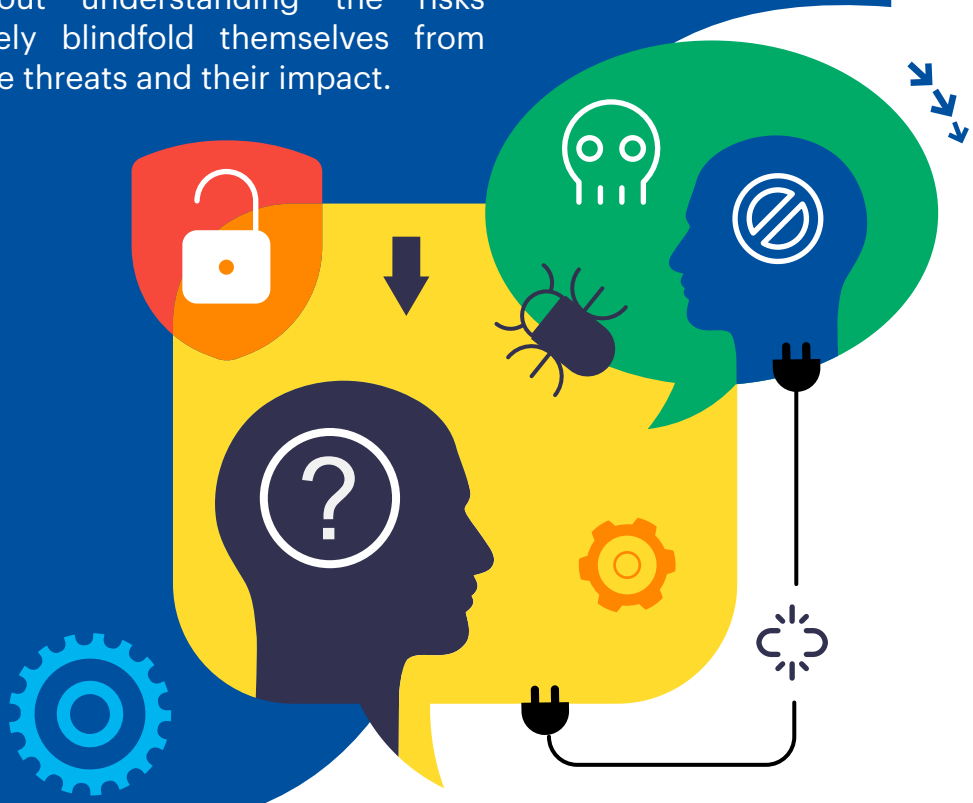
Benefits of Achieving Risk-Informed Decision-Making

Explicit risk integration into existing business planning and management routines will equip the organization with a natural vehicle to engage the cross-functional leadership team and entrench risk-informed business decision-making. Get this right and the benefits are compelling:

When planning and executing a business strategy, risk is typically viewed through the lens of constraint. However, these benefits highlight the power of adopting a proactive approach to risk; one that engenders strategic opportunities and provides a platform to successfully pursue them through risk-informed business decision-making.

Potential Pitfalls of Failing to Integrate Your Risk and Strategy Functions

The biggest risk is ignoring risk. Businesses that make their strategy a risk-informed function achieve clarity when navigating the risk landscape; whereas those that make decisions without understanding the risks naively blindfold themselves from these threats and their impact.



This short-sighted approach is tantamount to rolling the dice and hoping they avoid risks by pure chance – and exposes them to potentially crippling pitfalls:

- Restricts the ability to confront constraints that may be outside of the businesses full control but continue to prevent it from achieving its goals.
- Causes the business to conduct separate ERM and strategic planning processes involving the same stakeholders and similar topics.
- Disproportionately focuses on risks that relate to internal operations, while overlooking risks that are relevant to external stakeholders.
- Leads to the design of strategic goals, objectives and initiatives that do not anticipate barriers to achieving them.
- Failure to identify when a risk affecting a strategic goal or objective is likely to materialize.

Conclusion

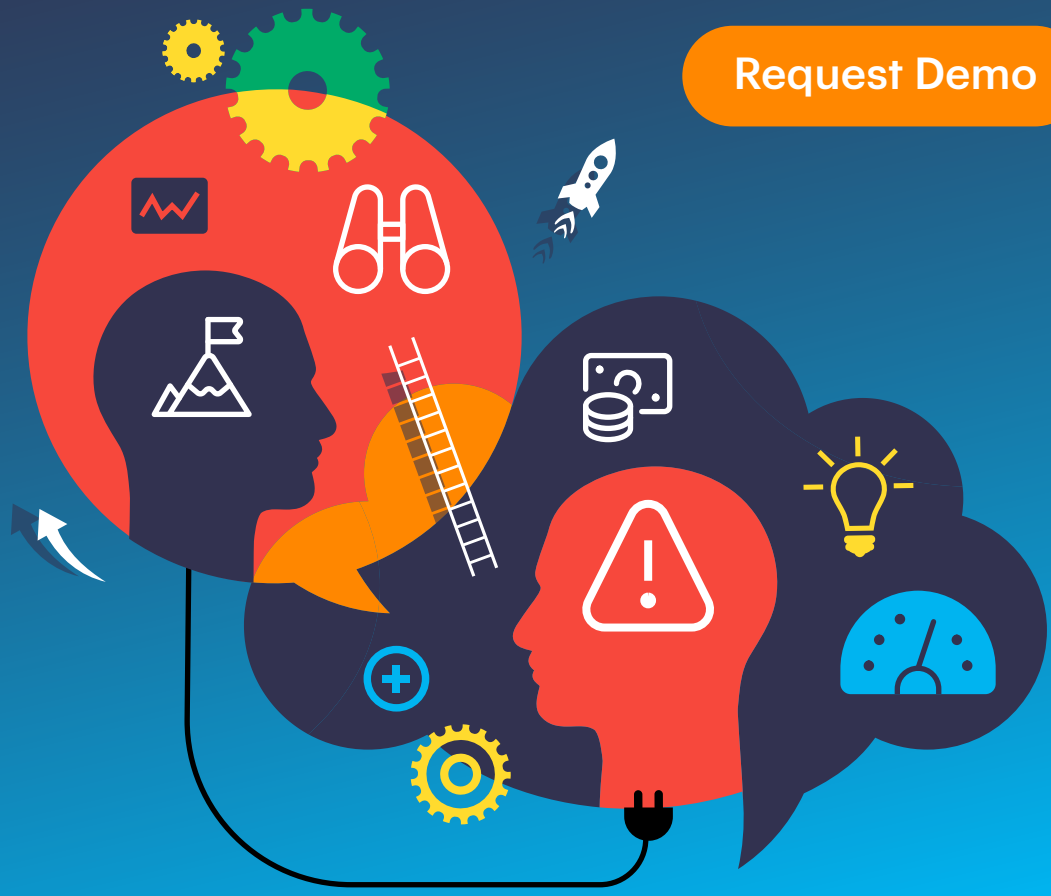
There is one constant in the dynamic world of business: risk. Every business has a choice to make in the face of this omnipresent force: bury its head in the sand and hope it goes away or don its armour and meet it head-on. Those that make important, costly and potentially damaging decisions in a state of uncertainty because they lack the necessary information put themselves under unnecessary pressure. Meanwhile, those that reinforce decisions with certainty by identifying and understanding the risks involved increase the likelihood of achieving desired outcomes.

The key to maturing decision-making is integrating ERM with the business strategy to create a risk-informed planning function. Strategy and risk are two sides of the same coin – with the execution of any strategy requiring some level of risk-taking. By aligning the two, the business will benefit from a symbiotic relationship between them – with the ERM program informing the strategy and the strategy informing the ERM program.

To build an effective risk-informed planning function, your business must embrace a holistic GRC software solution that has the power to consolidate disparate processes, systems and data sources into a single point of oversight. By choosing the right software partner to manage and integrate your risk management approach, you will be well-placed to deliver deep insight into the risk profile, status and performance of the entire business, while enabling integration and cross-functional interaction.

Camms' Gartner and Forrester recognized ERM solution can help your organization build an effective risk-informed planning function.

Request Demo



Camms.

Software to Change Tomorrow.

cammsgroup.com