

**Camms.**

Software to Change Tomorrow.

Business Intelligence  
for the C-suite:

**A New Vision**  
for Operational  
Risk Management



Perceptions are changing about operational risk management (ORM). So often in the past, C-suite executives discounted the function as an essential – but essentially, a checkbox-ticking – exercise. These same executives saw the risk management department as one whose function was solely to aggregate risk data and generate reports on it.

1990

In the 1990's, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) established controls to counter fraud. The COSO framework remains the standard for risk and control within most large organisations today. New approaches to increased and accelerating risk have only grown since COSO was first developed.

1999

In 1999, the Basel Committee on Banking Supervision first globalised “operational risk” as a term in conjunction with recommendations on banking laws and regulations.

2004

In 2004, Basel II linked operational risk to losses stemming from an organisation's people, processes or systems.

The ORM function has had an historical focus on responding to crises, developing worst-case scenarios and bringing visibility to the organisation's mistakes and problems. It's easy to see how organisations developed a negative perception of ORM.

Now, though, leaders can banish the negativity by elevating and enriching the ORM function. Operational risk managers already have the capability to deliver insights that will enable senior leaders to improve processes, make decisions, drive competitive advantage and identify the risks worth taking. By adding value through enhanced services like these, operational risk managers can support leaders in achieving business success and in defining and accomplishing strategic goals.

Fresh insights are generated when data and teams that are connected via systems promote a more expansive view of the business landscape – one that includes not only risk, but also new possibilities and opportunities. By using tools and methods that are already familiar to risk managers – in an environment of unified data and process – the same function that has protected organisations from risk for decades now can also deliver more valuable business intelligence for the C-suite.



# The Fundamentals of Operational Risk Management

**Operational risk** includes all risk related to doing business. These risks are incurred every day in the routine operations of any enterprise. Operational risk can span employee errors and misconduct, system failures, crimes like theft and fraud, trouble with third parties, broken processes, faulty controls and natural hazards like hurricanes and earthquakes. It also encompasses risks stemming from cultural, moral and ethical shortcomings and newer bias and ethics risks associated with innovative technologies like artificial intelligence and robotic process automation. A more distributed and interconnected business environment and increased reliance on third parties have also created newer forms of operational risk.

You may think there's nothing about operational risk that ever leads to a financial return, which makes it different from risks associated with markets or credit. And yet, operational risk is not only ever-present in every business process, it's also a frequent cause of financial loss and reputational damage.

**Operational Risk Management (ORM)** is a business discipline tasked with warding off the disruption and damage that would result if operational risk events occurred. ORM starts with understanding the organisation's appetite for risk and analysing the likelihood and impact of each risk an organisation faces. Effective ORM gives risk managers and C-suite executives more insight into an organisation's operational risks and provides information to enable fact-based risk-taking. This view — both detailed and broad — builds a strategy for organisations, enabling them to be more responsive to the expectations of customers, shareholders, regulators and other stakeholders. ORM also builds cultures of accountability, where risks can be escalated and openly discussed and prioritised to ensure they are addressed with the correct resources.

The importance of ORM has varied by industry, primarily driven by the potential impacts of operational risk within specific industries. In addition, regulatory authorities have introduced resilience requirements in a variety of industries. Financial services businesses are required by regulatory authorities to manage their operational resiliency; the healthcare and energy industries follow close behind with many mandatory regulations concerning ORM.

Organisations in any industry can realise the benefits of effective ORM, such as providing assurance to customers, shareholders and other stakeholders, creating a stronger risk culture (including more effective reporting) and delivering intelligence to support informed risk-taking. Organisations with rigorous ORM programs thrive because they remain resilient in the face of adversity.

ORM has focused on five key risk areas to build resilience. These risk areas reflect the growing complexity and accelerating rate of change in business environments.



## Cyber risk

Addressing the growing sophistication of cyber threats.



## Environmental risk

Anticipates extreme weather and other natural disasters.



## Reputational risk

Considers potential losses related reputational damage like lost revenue, increased costs and decreased shareholder value.



## Regulatory risk

Safeguards against missing some aspect of compliance in an increasingly complex regulatory environment. It also includes the risk of heightened regulatory scrutiny following a noncompliance event.



## Financial risk

Sometimes called liquidity risk — includes the prospect of losing money or having trouble with cash flow.

It's only recently that businesses are realising the knowledge, skills and tools that the ORM discipline has established could readily lend themselves to a broader and more positive variety of business situations – like developing corporate strategy, identifying opportunities and supporting calculated risk taking.

Even as they manage and monitor these risk areas, ORM leaders are on the brink of a new opportunity: bringing ORM's traditional strengths, tools and expertise to an expanded remit that includes delivering business intelligence to the C-Suite. Addressing and automating ORM's most common challenges through shared systems and departmental collaboration clears the way to an expanding role for ORM.





# Key Challenges in Operational Risk Management

Even as the ORM function stands ready to fulfill its role as strategic consultants to the C-suite, it faces an abundance of obstacles. There has never been a time when ORM was more essential, yet ORM leaders face significant challenges to their effectiveness:



## Diversity of risks.

Trends like globalisation, competition and new technologies result in risks so varied that no single approach suits all of them. The number of risks has grown and risk types have become more diverse and span across multiple departments. These risks include active regulatory environments, third-party risk and cyber threats.



## Lack of role delineation.

The ORM function is often conflated with functions whose objectives overlap, like compliance, information technology, cybersecurity and legal – sometimes resulting in gray areas where roles can become confused and critical responsibilities overlooked. This lack of role clarity is also confusing for stakeholders who need to know the roles of each of these functions, how to interact with each of them and how information flows among them.



## Disjointed processes and systems.

Historically stemming from a reactive and crisis-driven environment, ORM processes and systems have grown organically and sometimes remain disjointed to this day. What's often missing is a cohesive, forward-looking governance structure that defines, delineates and coordinates among ORM processes and systems.



## Inadequate metrics.

Operational risk is notoriously harder to measure and manage than financial & credit risk, where risks can be computed as amounts and percentages. Until recently the diverse and qualitative nature of operational risk has complicated the production of meaningful metrics. Now though, modern risk management systems are yielding more data; capturing it consistently across multiple departments to enable comparison of results and identification of trends.

When it comes to ORM data availability is just the beginning: applying analytics to risk data completes the shift from qualitative perceptions to data-driven risk detection, real-time monitoring — and business intelligence.

Diversifying expertise, clarifying roles, focusing on future threats and maximising the potential of modern ORM systems will help risk leaders prevail over challenges and position the ORM function to expand its focus to encompass strategic business intelligence. Establishing a best-practice ORM framework will facilitate these achievements.

“ ORM has recently become capable of assembling data to form insights that support organisational resilience and strategic decision-making. ”





# Building an Operational Risk Framework

No organisation can begin harnessing its ORM data to form meaningful insights without developing its operational risk framework first. It's a journey each organisation must take for itself, because every organisation differs from others in size, complexity, industry, culture — and risk tolerance.

## Formulating the ORM Framework

Effective ORM frameworks grant organisations the flexibility to respond to changing regulatory and stakeholder expectations. Regardless of any business' unique situation and particular risk tolerance, its ORM framework should consider current conditions and anticipate changing expectations.

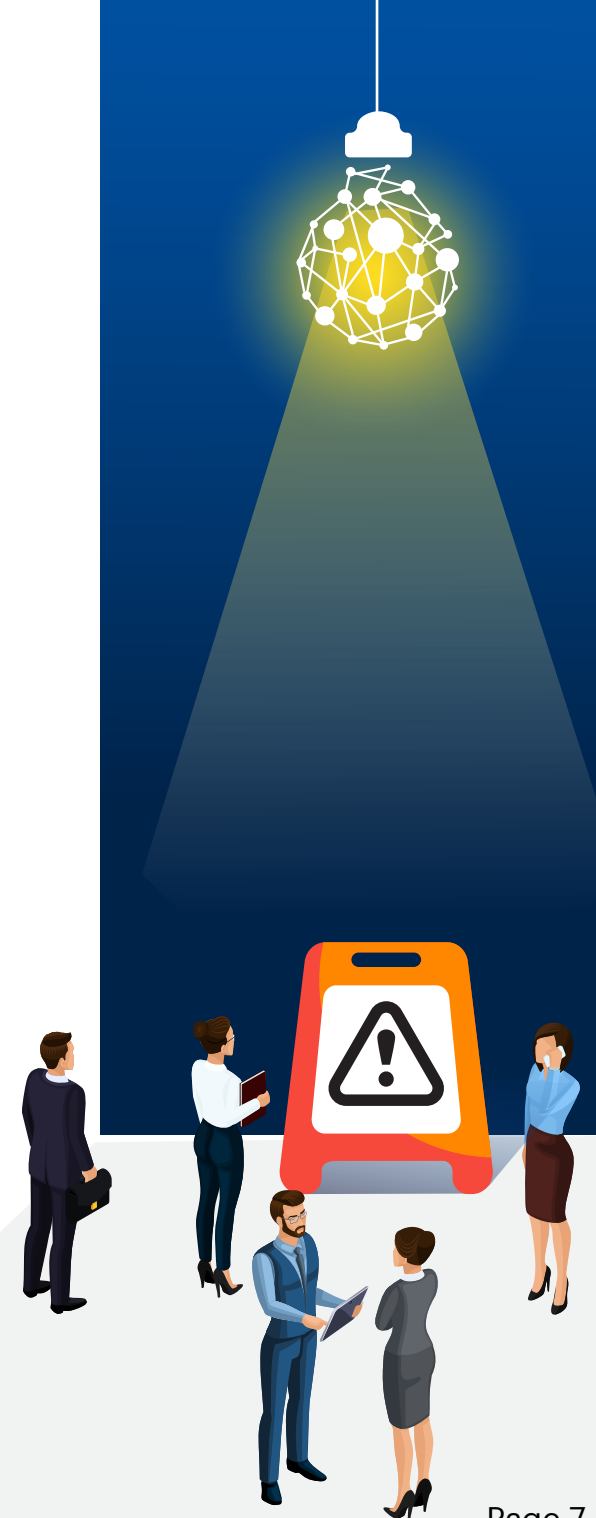
The following activities will result in an ORM framework that meets the organisation where it is right now, and advances it to a more resilient, risk-aware culture and a more responsive risk stance:

**Assess risk culture.** Strong risk culture demands transparency about risk issues among senior leaders and business units. It includes leadership's dedication to risk management, even at the board level. Helpful questions include:

- Does the organisation welcome risk escalations and debate about risk decisions from multiple viewpoints?
- Does it accept questions about the effectiveness and risk levels of its current processes?

**Establish a methodology for assessing risk.** Use data to develop analyses and models that support business decisions around risk. Make sure the processes via which measurements are made are transparent throughout the organisation. Use data to clarify when exposures are shifting, so the organisation can take action where needed.

**Evaluate the strength and effectiveness of current controls.** Modify controls when necessary, developing controls that align to risk probabilities and impacts. Clarify risk responsibilities and protocols for risk measurement. This is especially critical when accountability is shared across departments.



**Make ORM intrinsic to all business processes** – don't allow ORM to be viewed as a sideline to other operations activity.

- Risk teams should develop strong relationships with business units.
- Partner with the business units to address risk events in a timely way, escalate them as needed and report on risks according to predetermined communication plans.
- Make business managers accountable for risk mitigation within their own operations. Incorporate analysis of potential risks and any cost associated with controlling them into budget and profitability forecasts of each business initiative.

**Include risk management principles in every general management role.** Implement training to ensure leaders have a broad understanding and application of the organisation's risk framework.

**Establish how ORM will be governed.** Consider the staff, systems, policies, processes and controls that will support decision-making related to operational risk. This is an opportunity for risk leaders and the C-suite to connect and communicate with the entire business about the importance of risk management.

**Determine how the ORM function will communicate with stakeholders.** Include specific media and messaging for different audiences under different circumstances. Notifications are certainly in scope; continuous promotion of risk awareness should be, too.

**Set up structures for reporting** Give special emphasis to risk communication and escalation. Reporting processes should be supported by technology that provides differing levels of information depending on the responsibilities, interests and risk appetite of different recipients.

**Build skills within the ORM team** based on the organisation's industry, business model, geographical footprint, business climate and risk trends. Reassess the skill mix periodically to keep ORM skill sets aligned with the business environment.

## Setting a Risk Tolerance

How much risk can an organisation accept? Determining risk tolerance and articulating it is central to accounting for risk in business decisions. Initiating candid conversations about risk tolerance will clarify the level of risk the organisation can accept. Risk tolerance statements encapsulate leaders' philosophies about taking and managing risks. This is not a calculation: the organisation's senior leaders must state "minimum and maximum levels beyond which the organisation is unwilling to lose."

## Using Risk as a Competitive Differentiator

Beyond establishing an organisational risk tolerance and an ORM framework, leaders can position ORM to add business value.

- Instead of risk prevention, think in terms of enabling the calculated risks that accelerate growth.
- Use the power of ORM's data so stakeholders can voice independent views backed up by data without fear of retribution.
- Enable the C-suite to pinpoint accountabilities, control failures and losses.
- Use ORM information to support more effective articulation of the "tone at the top" to enable cultural changes driven by facts.
- Grow organisational awareness of operational risks associated with the entire product lifecycle to make better decisions about product offerings.



# Building a Risk-Aware Culture

In a strong, risk-aware culture, everyone in the organisation understands that managing risk is an essential part of their responsibilities and considers it in their everyday activities. A risk-aware culture can only emerge when role models display the desired behaviors and this leadership echoes through the business enabling individuals to link risk management to their own roles. Over time, modelled behaviors instill the values and beliefs that foster risk awareness.

Policies, procedures and other communications articulate expectations of risk-aware, conscientious behavior. When this behavior is recognised and rewarded, more individuals are encouraged to model it — and to a greater extent. Even small gestures of recognition carry symbolic significance and help to instill strong risk culture.

To begin to strengthen risk culture, it helps to consider the organisation as it is today: ask questions about current attitudes toward risk and evaluate the organisation's approach to risk management. Evaluate whether attitudes and behavior align with the risk tolerance statement. Assessing the current risk culture can begin with questions like:

- Are leaders displaying the right behavior around risk?
- Are employees receiving consistent and useful messaging related to risk?
- Does the organisation share a common language for discussing risk, including terminology and measurement?
- Are managers and staff open about discussing risk, or do they fear raising risk-related issues? Are they prompt about raising issues?
- Are managers and staff clear about their own risk accountabilities? Are they skilled and trained to manage those accountabilities?
- Do managers and staff bend rules to achieve their goals?
- Do managers with primary risk accountabilities have sufficient authority to take action when needed? Are those managers knowledgeable about risk management and engaged in risk management activities?
- Does the organisation have a risk tolerance statement and an ORM framework? Are the organisation's strategic goals aligned with its stated risk tolerance? Is management of risk a measured aspect of leaders' and the organisation's overall performance? Is the framework regularly reviewed and broadly understood?
- What tools do leaders use to gauge the effectiveness of the ORM program? How could these tools be made more effective?



Operational risk managers are on the front line of shaping risk culture, but they have to be supported by their leaders and colleagues. The support of risk-adjacent functions like legal, security, fraud management, business continuity, compliance, insurance, cyber security, vendor management and environmental health & safety are especially important allies in building risk-aware culture.

While risk management is often a small department, risk affects every aspect of business operations. Therefore, ORM leaders should seek out partners and advocates in all departments to maximise influence. ORM leaders can collaborate with the business to build a culture focused on organisational success. Developing strong relationships with leaders and colleagues helps build a results-driven risk culture.

Risk managers can consult with colleagues to guide them through their decisions about risk and help them to navigate options for addressing it, using organisational agreements about risk tolerance as the guide. Risk managers can also help colleagues develop the holistic view of operational risk that's essential to making informed business decisions. Shared systems help heighten awareness of risk and of ORM effectiveness by bringing teams together and engaging all departments to provide centralised risk information in an automated way.

## How Automation Drives a **Rapid, Focused Response**

A broad and thorough understanding of ORM throughout the corporate culture is to any organisation's advantage. Bringing all risk data together into a single system enables meaningful decisions and facilitates the involvement of everyone responsible for identifying and responding to operational risk.

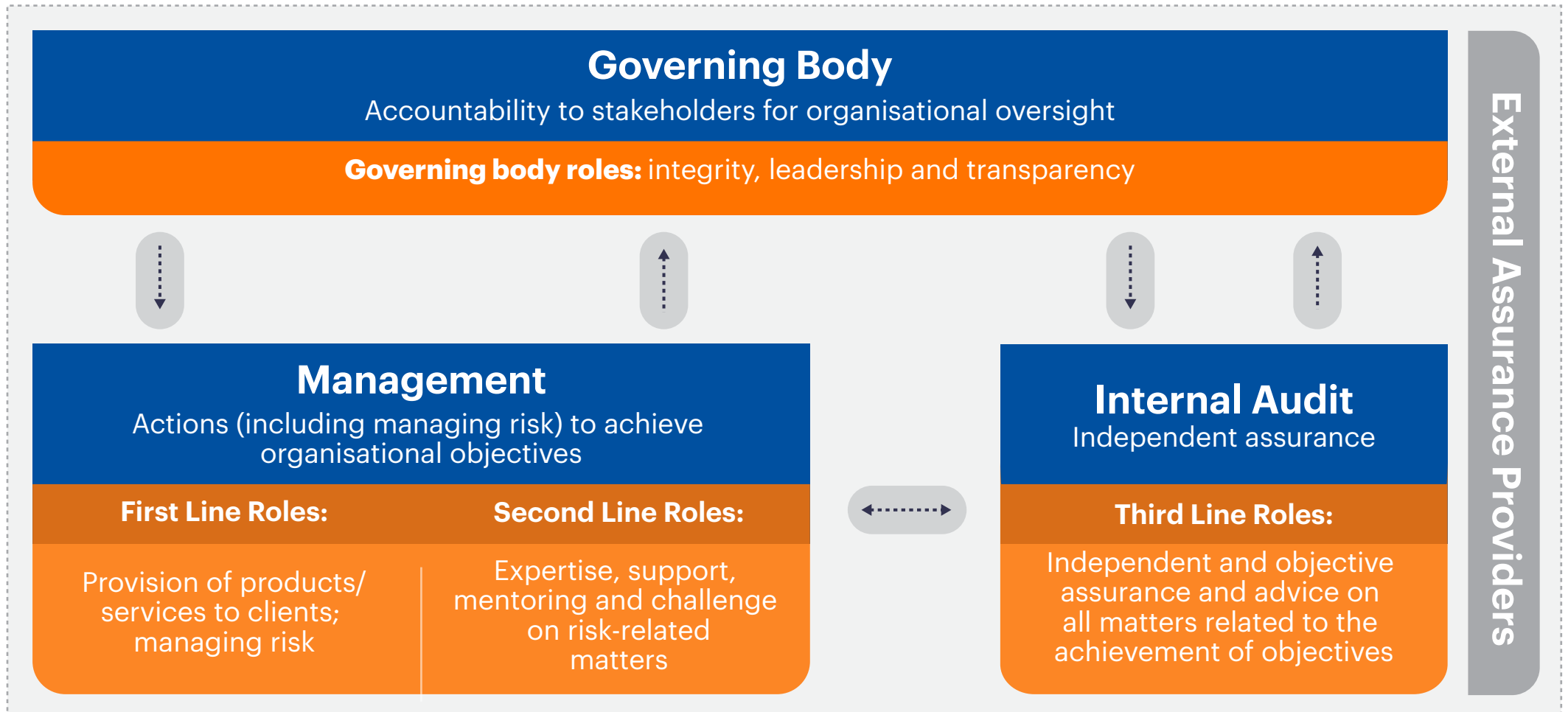
Organisations are turning to information systems to integrate and optimise ORM activities.

Automated risk management fosters collaboration throughout the business and supports maturing of risk management processes overall. Workflows, centralised storage, dashboarding and reporting unify processes and enhance the visibility of operational risk information.

“ As ORM requirements grow in complexity and volume, organisations are turning to information systems to integrate and optimise activities. ”

## Automating Defense

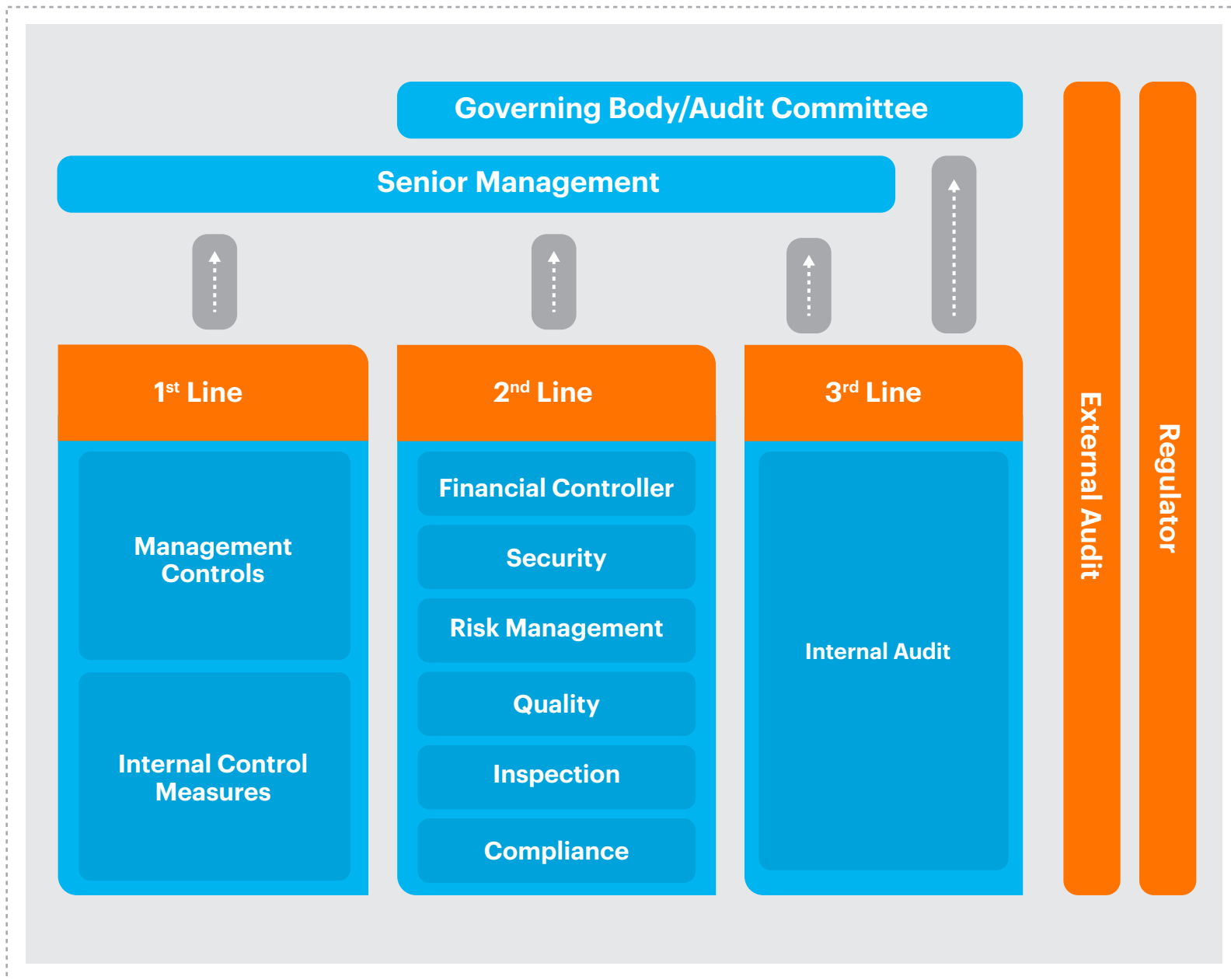
As ORM has evolved as a discipline, so too has the traditional Three Lines of Defense risk methodology. In 2020, the Institute of Internal Auditors (IIA) updated its model to move beyond defensive maneuvers and emphasise a more active approach to risk management. The model is now known as the “Three Lines Model” — significantly, “Defense” is gone from its name.



The updated IIA model incorporates a governing body and delineates the roles of executives and internal auditors. Guidance for using the model emphasises interaction, communication and collaboration.

It stresses that working together across both the first- and second-line roles of management and internal audit is essential to prevent unnecessary duplications, overlaps, or gaps.

## Automating Your First Line



When businesses use GRC technology to automate the first line and put controls in place, they increase risk visibility. Incidents that reach the organisations risk tolerance can be centrally captured. Alerts can be configured for automatic distribution to the required stakeholders. Problems can be made visible the moment they arise, freeing second line resources — that is, finance, security, quality, inspection, compliance and risk management — to focus their expertise, support and monitoring on matters related to risk events. This is where modern risk management systems like Camms contribute significant value to operational risk management and control processes.

# The Top Ten Operational Risks

Risk.net's ranking of 2021's top operational risks demonstrates the rapid pace of change — and intensification of risk — that COVID and digital transformation have wrought. As challenges intensify, risk leaders have more to manage in their ORM programs. [Risk.net's top ten risks](#) highlight the need to track and analyse more data and trends to avoid damage and disruption:

1

## IT disruption risk

This includes everything from blackouts to deliberate malfeasance from outside parties. The pandemic created new exposures to cyber-attacks, third-party risk and hackers. Threats from ransomware have also risen to record levels.

2

## Data compromise risk

As more staff work remotely, the risk of data breaches has risen. Accelerating adoption of cloud platforms is leading more risk managers to intensify governance and monitoring, as well as heightening cyber security controls to protect data and comply with data privacy regulations.

3

## Resilience risk

The events of 2020 revealed that planning for business continuity and operational resilience had not included anything on the scale of the global pandemic. Businesses encountered unprecedented market volatility and supply chain disruption, while they struggled to equip staff for secure remote work.

4

## Theft and fraud risk

Theft and fraud is ever present and is evolving into new, more insidious forms, facilitated by the pandemic and new opportunities for bad actors enabled by advanced information systems and heightened interconnectedness.

5

## Third-party risk

Vendor risk management was exacerbated by the pandemic as on-site inspections of partners became impossible. Some organisations' overseas outsourcing relationships were disrupted by local shutdowns. Almost every business relies now on vendors for cloud storage, remote access, video conferencing and other services, keeping third-party risk management at the forefront of risk issues.

6

## Conduct risk

Risks relating to business conduct are harder to see now that remote work has become the new norm. Risk managers had previously relied on the social environment of the workplace to identify via informal interactions and signals.



7

### Regulatory risk

Regulators change rules and expectations, increasing the likelihood of inadvertent violations. However unintended, the fines and reputational damage to organisations remains a real hazard.

8

### Organisational change risk

Business leaders were forced to restructure and introduce new operating models following COVID's first wave. Leaders learned that staff often prefer remote work, customers are content to take business online and savings on real estate and other overhead items are significant. As businesses seize new opportunities, strong governance and change management will be even more essential.

9

### Geopolitical risk

Some nations shuttered businesses due to COVID or experienced disruption due to war and internal strife, complicating international trade.

10


### Employee wellbeing risks

Concerns over employee wellbeing have increased as individuals struggled with rapid shifts to at-home work, while also suffering fear of infection for themselves and for loved ones, leading to decreases in productivity and morale.




# Automating ORM using specialist GRC tools


Systems that support a more connected approach to ORM enable an environment where risk data from across the entire organisation is readily available to support strategic decision-making. These systems promote a cohesive view of risk — and opportunity — throughout the enterprise. They enable teams to manage and monitor action plans, maintain risks within established tolerances and manage the status of projects and their associated risks. They facilitate coordination of risk incident responses. Through the monitoring of trends, they deliver predictive views of emerging risks. Many GRC solutions offer approaches tailored to specific risk issues:




Advanced analytics capabilities help ORM departments to delve into their data to spot trends and anomalies. Analytics supports advanced operational risk detection by revealing risks faster and reducing false positives.




Machine-learning (ML) helps focus ORM resources on situations that require human intervention by replacing rules-driven alerting systems. ML can also analyse and identify emerging threats more sensitively than rules-based triggers; it can also apply unsupervised techniques to spot instances of fraud and analyse new customers' and trading partners' profiles faster and in greater depth.




Natural-language processing can be applied to call surveillance.




Automated control monitoring can identify risks quickly based on preset rules and alert the relevant stakeholders.




Advanced modelling features promote a risk-based approach to vendor selection and assessment by quantifying third party risk. Modelling also improves business continuity planning.



Purpose built GRC tools offer best practice risk frameworks, enabling businesses to quickly define and prioritise their key risks and define tolerances.



GRC technology helps bring business functions together to share risk data. Using API's data can be captured consistently and pulled into a centralised system providing a holistic view of risk.



Many GRC providers offer functionality to manage other risk areas like, cybersecurity, vendor risk, health & safety and enterprise risk in the same solution alongside operational risk giving business deep insight into their risk profile and bringing teams together.

Beyond applying advanced technology to classic ORM applications, modern risk management software can help ORM teams apply all they know to business resilience and corporate strategy as part of a mature ORM program.

# Developing and Maturing Your ORM Program

Modern organisations are experiencing accelerated technological change and expanding data availability, and they're responding with new, data rich business models. Technological change is driving new ways of serving customers and managing operations. Ever-growing data sets need governance and management to transform them into business intelligence assets. Organisations benefit from these new possibilities and as they do, ORM must stay current with the technological and process trends that contribute to an evolving risk landscape.

Even as technological change engenders new risk, it is also enables the maturing of ORM as a discipline. ORM can become more targeted and efficient than ever before. It can also become better-integrated with corporate governance and strategic decision-making. No wonder ORM leaders are looking for better tools.

Unlike the corrective approach that characterised ORM at its inception, modern, mature ORM looks ahead, emphasising resiliency and hardening organisations against critical vulnerabilities and unlocking opportunities. Mature ORM programs leverage operational data to measure risk. They're shifting away from subjective self-assessment of risk to engage in automated, real-time monitoring. They're shifting away from a proliferation of controls and toward data-driven risk measurement, advanced detection tools and techniques and in depth dashboards and reports.

More-mature ORM programs can address the challenges that impact the organisation's bottom line. Empowered by centralised risk data, monitoring and automation, ORM teams can expand their roles to add greater value as partners to the business. They can shift from devising controls to providing their risk management expertise to new challenges like the design of innovative processes, products and business models. With new efficiencies afforded through advanced technologies, risk leaders can make themselves more available to assist senior leaders with evaluating operational strengths and vulnerabilities.

“ More-mature ORM teams are positioned to deliver more value to their organisations, helping the C-suite to take calculated risks, design better-informed strategies and pursue opportunities so the organisation can perform at its best. ”

## ORM Maturity Supports an Expanding Role

Broken processes are the root cause of much of today's risk. Disruptions of customer relationships, lost revenue, reputational damage and more can result when processes fail. ORM can help C-suite leaders and risk managers evaluate whether processes are effectively designed for both routine and extraordinary circumstances, and whether they result in consistently positive outcomes. It can help leaders determine whether change management processes anticipate challenges to prevent disruption.

When ORM is linked to the entire business and utilising automated workflows and controls within a specialised tool, ORM departments can turn their focus to improving process efficiencies, and identifying opportunities for improvement and growth – matters that go beyond the traditional role of ORM. These expansions are only possible when ORM teams are armed with the right tools to collect the right data and feel able to use the insights to influence C-Suite decision making.



Mature operational risk programs must consider human influence. Employees are everything to a business. That said, employees, contingent staff and third parties also have the potential to disrupt and damage organisations through ignorance, transgressions, abuse of insider information and malicious noncompliance. Access to information leads to information leaks. Inaccuracy and negligence contribute to error rates. Incomplete understanding of the organisation's offerings leads to misinforming customers and prospects. Poorly designed incentives can create pressures to sell or process transactions in an irresponsible way. Detecting, quantifying and prioritising human-factor risk is an even greater challenge for large complex international organisations. Maturing ORM promotes real-time detection of risks related to employee behavior, resulting in swifter intervention. Culturally, this will call for greater agility and increased reliance on collaborative, interdisciplinary teams.

Organisations continue to rely on subjective detection of risk via self-assessments and control reviews. While effective in some cases, these approaches can't stand up to detecting new cyber threats, or events that are low in probability but high in potential impact. Mature ORM teams have reconsidered detection approaches and use data analytics to make sense of the sea of structured and unstructured data that is available to them. Real-time testing of processes, controls and metrics can highlight volume spikes in key transactions and similar indicators of risk. Targeted systems can detect unauthorised transactions including fraud and help ORM teams track staffing levels, processing times, inventory thresholds and more, by spotting connections within diverse data and identifying both risk and opportunities for improvement. That's why leveraging modern technologies like data analytics to detect issues and report in real time is a signifier of maturity in ORM.

The variety of operational threats calls for specialised expertise – in technology, data and in new and emerging vulnerabilities. Effective risk oversight calls for current knowledge about how processes and systems can be compromised. Risk leaders, therefore, are recruiting talent and developing skills in-house to make the best use of advanced analytics. That's why risk leaders who are motivated to mature their ORM approaches are training and recruiting ORM team members to meet new skill requirements.

“ Mature programs give op risk teams the capacity to grow beyond risk management and enlarge its focus on operational excellence and resiliency. ”

Whereas the function had once focused on detecting and reporting risks, the mature ORM role that's emerging now applies its substantial arsenal of tools, models, language and techniques to support resiliency and strategic decision-making in all of a business' operations. ORM maturity and modern risk technology enable this, but to affect this expansion, leaders must also consider the organisation's perception of the ORM function.

# A Department of Business Intelligence: Changing Organisational Perceptions of ORM

ORM's role is becoming more strategic – and of critical use to the C-suite. ORM teams have started equipping senior leaders with the business intelligence they need to determine what risks are worth taking.

“ Since emerging as a business discipline two decades ago, ORM's role has evolved from risk preventor to enabler of the best kind of risk: calculated risk. ”

Calculated risks maximise opportunities, improve processes and decisions — and drive competitive advantage.

Norman Marks, a global thought leader in risk management, recently described the problem of outmoded perceptions of risk management this way:

**“Too often the risk team is seen as the department of 'No'; the department that quite literally stops people from doing what they want to do and diverts them from what they see as running the business.”**

ORM leaders can educate the C-suite about how risk management tools, models, language and techniques can inform strategic planning and corporate goal-setting. Supported by this knowledge, the C-Suite can begin to rely on ORM teams as providers of expertise and information: extracting the fullest value from business intelligence assets they already have on hand. Thus prepared, leaders can exploit the skills and knowledge ORM can deliver to profit from new opportunities and take calculated risks in support of better-informed strategies.

The surest way to change perceptions is to perform in accordance with the new vision for ORM. ORM teams can help C-suite executives establish earlier whether the organisation is on track to achieve its objectives and they can do it with greater accuracy. By making use of all ORM already knows about monitoring and metrics, risk managers can start helping executives gauge progress toward objectives as easily as they track closure of gaps today. Executives can come to rely on ORM to deliver intelligence that supports strategic decision making, offering a better balance of intuition and reasoning with data analysis and statistics.



To derive the greatest-possible value from risk data, ORM leaders will want to link data and process across functions so that risk intelligence, compliance policy and corporate strategy are unified. Once unified, these considerations can be addressed together more easily, resulting in fresh analyses, insights and visibility into opportunities that had been lost in a sea of information. Integrated platforms that support governance, risk, compliance and strategy together enable shared intelligence. Systems like Camms aligns strategy with governance and risks to empower agile and competitive enterprises. Centralising and analysing data allows C-suite leaders to make the most of an organisation's information. As a result, they make better decisions to grow the business.

Rebranding ORM through both a broader use of its traditional methods and application of modern technology corrects a frequent misperception that the ORM role is a negative one – that risk managers exist to inhibit business units in pursuit of their goals. ORM can transform itself into the function of business intelligence. ORM teams are now positioned to leverage all to the data they have to deliver information and opportunity – and to identify the risks worth taking for senior leaders.

## From Crisis Response to Operational Excellence

ORM is shifting now from an historically reactive focus on crises to a modern, forward-looking emphasis on offering consultative services to improve the C-suite's strategic decision-making. Much of this transition reflects the maturing and modernisation of the ORM function, including increased availability of modern information technology to complement an already-robust arsenal of tools, models, frameworks and techniques.

Mature ORM supports superior business decision-making. Combining diverse data sources into a single system and then applying advanced data mapping capabilities frees risk managers to contribute at a more strategic level.

Leveraging the best technologies to evaluate ORM data and consolidate it into a single source of truth provides the support that the C-suite needs to lead with vision. When changes occur – as they always do – leaders can make decisions informed by a complete picture of the risk climate and their position in it. New suppliers, new systems, new models of business can be viewed in the context of a realistic, real-time operational risk profile.



### Providing Business Intelligence to the C-suite

Leaders are redefining what value ORM can deliver within their organisations. They are reinventing the ORM function, expanding it from tactical response planning and risk data reporting to encompass a key role in providing consultative services to senior decision-makers. This richer, expanded role will enable C-suite leaders to make better-informed decisions, drive competitive advantage, improve processes and identify risks worth taking to achieve success and deliver on strategic plans.



# Camms.

Camms offers a cloud based SaaS solution to manage your Governance, Risk & Compliance program. The solution uses a modular approach, allowing organisations to scale and mature their operational risk management processes at their own pace. The Camms solution offers best practice operational risk functionality including:



## Risk Registers

Camms offers multiple risk register views for logical comparable risk data from across the business so you can visualise your key risk indicators.



## Audit management

Schedules and manages internal and external audits and formalises the results and required actions.



## Incident management

Facilitates incident and near misses reporting in real-time, and the investigation process post-event.



## Risk Assessments

Perform best-practice risk assessments in line with ISO 31000 and calculate the likelihood of occurrence and generate risk ratings.



## Stakeholder dashboarding

Intuitive functionality provides executives and the board with key operational risk information when they need it.



## Analytics and reporting

Built-in dashboards and standard reports provide critical risk insights and executive reporting.



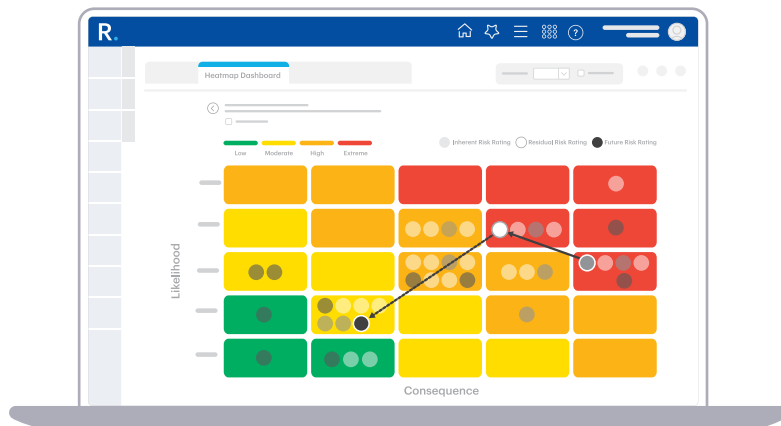
## API integration and library

Seamlessly integrates all Camms software with any existing systems containing risk & compliance metrics and transfers data both in and out of our solutions.



## Risk Appetite

Define your organisations risk appetite and operationalise your risk tolerance framework.



Adopting a comprehensive approach to managing risk will facilitate the transparent flow of relevant information from the top-down, and the creation of a proactive risk aware culture from the bottom-up – empowering the right people to make the right decisions at the right time. Never has this been more important to a business’s current and future success. As risks become more diverse, businesses need a risk management solution that can collect and aggregate risk data from across the entire organisation. The Camms solution enables stakeholders from across the business to feed into the risk management process, providing comprehensive data to not only mitigate risk but provide insights to uncover process efficiencies and opportunities for growth.

Business Intelligence  
for the C-suite:

# A New Vision for Operational Risk Management

Camms business solutions have the power to integrate meaningful risk, strategy, project, and people solutions, helping you make the right decisions, manage risks, align talent and focus on what matters.

**Our team would love to learn about your company and its Operational Risk and GRC needs. Request a demo with us today!**

[Request Demo](#)

## Camms.

Software to Change Tomorrow.

[cammsgroup.com](http://cammsgroup.com)

