Camms.

Whitepaper

8 Surefire Ways to Improve Your Risk Management Programme

Companies who adopt a proactive approach to risk management are well prepared to control and respond to risk events.

Organisations face a diverse range of risks. These can range from operational events like system downtime, loss of power, and fraudulent activity to regulatory risks relating to non-compliance. Strategic risk must also be monitored – including competitor activity, the launch of rival products, and technology advancement & trends.

Whether strategic, operational or compliance driven, risks can pose some level of threat to an organisation, and escalate, if not managed effectively. Companies who adopt a proactive approach to risk management are well prepared to capably control and respond to risk events.

Taking the first steps towards a proactive, effective risk management plan can be overwhelming. To get started, Camms encourages all organisations to consider four high level priorities:

Engage Stakeholders:
Risk teams must engage with stakeholders across the organisation to get visibility of the full spectrum of risk. This can involve having risk champions from different teams and assigning ownership for monitoring risk and testing controls and their effectiveness.

Get Visibility:
Centralise risk data to get a holistic view. Capture data from risk assessments & checks and use operational & transactional data from various systems and data sources to understand the likelihood of risk and anticipate hazard factors.

Remediation & Response:
Develop a risk framework to easily, categorise, rate, and prioritise risk. Implement effective controls to mitigate known risk and guide effective, rapid, comprehensive reactions to risk.decisions.

Reporting:
Ensure your risk data provides executives & managers quick, accurate information, to drive informed business decisions. Ensure you are able to report on risk at a functional level and a group level to suit all audiences.

Once these four priorities are understood by key stakeholders, and you have sufficient processes in place, it is time to explore 8 surefire ways to improve your risk management programme.

8 Surefire Ways to Improve Your Risk Management Programme

1 Standardise Your Risk Rating Methodology

Organisations must manage a varying array of risk across different departments & sites, with each one varying in likelihood, severity & impact. To build a strong risk management framework, organisations must establish a common set of definitions to identify, assess, categorise, and rate risk. Imagine managing a risk incident in which one employee had rated the risk as 'moderate' but another employee had rated it as 'major'. A standardised risk rating methodology is the only way to remove subjective opinions, unintentional bias and to identify and manage those risks that are most important to the organisation. This ensures a risk is rated and categorised in the same way, which ever site it occurs at, this will ensure risks are prioritised correctly and efforts, controls, and budgets can be allocated towards reducing the most critical risks.

Focus areas:

Identify risk categories that best match the environment in which the organisation operates and then develop objective consequence and likelihood descriptions. Ensure that the risk impact matrix accurately reflects the type of organisation you have. Train the teams that are involved in identifying, assessing, rating, reviewing, documenting, and reporting risk on the agreed framework so that all stakeholders are aligned.

2 Assign Responsibility for Risk

The 'three lines of defence' concept is crucial to ensure efficient management and ownership of risk - adding a layer of essential governance to the process. The first line of defence is there to ensure functional accountability on the front line where the risk is likely to happen, this can either be automated through internal controls or risk assessments or can involve checks performed by the risk owner or those with accountability for the risk area. The second line of defence requires management oversight, and usually involves the risk & compliance team, and the third line of defence demands independent assurance usually involving an internal audit team.

Some organisations make risk management the sole responsibility of a dedicated risk management team, however this can restrict an organisations view of risk. Risk management works best when it is a clear, integral part of everyone's role. Risk is everywhere. It is impossible for a small risk team to identify, assess and respond to every risk event without involvement from the wider organisation.

Taking an organisation's approach to risk further than just a dedicated risk team requires planning, employee engagement and support through training and involvement. A strong risk management plan will involve employees across the organisation feeding into their risk management programme.

Risks and controls can be owned and managed by any employee in the organisation and risk assessments can be completed by those on the front line. It is only by involving the wider organisation and broadening the scope of risk that an organisation can build a realistic picture of enterprise risk. GRC software can facilitate this process. Employees of any level can log into the platform and complete tasks like risk assessments, control checks, and actions. Each employee will have access to their own dashboard to see their upcoming and overdue tasks & actions, they will also see snapshots of relevant reports & metrics. Dashboards will vary depending on roles & responsibilities.

This approach enables a much wider audience to feed into the risk programme, providing more data for risk teams & boards without employees having to touch the actual risk register. Risk related tasks just become part of their daily routine and automated notifications & alerts ensure tasks are completed promptly.

Focus areas:

Survey attitudes to risk across the organisation. How do people perceive risk? What do employee opinions reveal about awareness of and responsibility toward the management of risks? Are people aware of both strategic and operational risks? With these insights, design a programme of awareness and upskilling on risk management, appropriate to the roles and responsibilities in the workplace.

Design a process where employees can feed into the risk management programme and 'own' risks and controls and perform checks & risk assessments. This is usually best done using a GRC software solution where every employee can access the system and complete risk assessment templates and control checks. Automated workflows then ensure risks are escalated and resolved promptly. It also gives senior management a live view of risk status and problem areas so they can take action. Make sure employees, especially those at senior levels, understand their role, responsibilities, and accountabilities for risk management - and the implications if these are not undertaken effectively.

3 Capture Sufficient Accurate Risk Data

The success of a risk management programme relies on having access to the right data enabling teams to understand risk exposure and control effectiveness and identify & resolve problems quickly.

Therefore, once you have established your key risks and compiled then into a risk register, you need to consider which data will be used for your Key Risk Indicators (KRIs). That data might be results from various risk assessments, it might be transactional or operational data held in operational systems & spreadsheets, or it might be data from regular checks carried out by individuals. What ever that data may be, you need to work out how it will be captured consistently and centralised so it can be easily reported on.

GRC software can automate the collection of risk data. Online forms can be used for employees to complete risk assessments, questionnaires, and surveys with all data feeding directly into the platform. GRC technology also offers API integrations with other internal systems, data sources, and spreadsheets – enabling organisations to pull operational & transactional data into the platform to monitor risk levels. Having these integrations ensures a single source of truth for risk data and cuts out admin and data duplication tasks that can result in errors.

Focus areas:

Build a comprehensive register, define what your Key Risk Indicators (KRIs) are, and establish what data you will monitor to track risk levels. Ensure data is captured regularly and consistently across different sites - inconsistent data results in inaccurate reports that lead to mis-informed decision making. Use online forms with strict data governance rules, using predefined dropdowns, formatting rules, and mandatory fields. GRC technology is a great way to implement data governance, it enables risk teams to customise forms, fields, and dropdowns to ensure data is collected accurately. Automated workflows can even be set up to send out regular online risk assessments with all data feeding directly into the platform - meaning it can easily be reported on at any time. Risk assessment forms should be customised to suit each risk type and business area.

4 Formalise & Automate the Risk Assessment Process

Risk assessments are an important part of any risk management programme. Different areas of the organisation and different risk types will require very different risk assessment forms. It is important to use best-practice risk assessment templates which can then be further customised to meet the individual requirements of the organisation and to cover any regulatory requirements.

Most organisations use GRC software to automate the risk assessment process. Best-practice risk assessment templates are often available within the platform, and they can be further customised to meet any bespoke needs. They usually offer the option to upload photographs, documents, and URLs to ensure all relevant information is captured. The forms contain data governance rules like searchable drop downs, text formatting guidelines, and mandatory fields to ensure information is captured consistently - ensuring it can be easily reported on later down the line.

Most systems offer workflows to automate the risk assessment process. Automated notifications are sent to the relevant stakeholders asking them to complete the online risk assessment with clear deadlines. All outstanding forms are chased by the tool and reminders are sent. Data from the risk assessment forms feeds directly into the platform enabling leaders to easily identify high risk areas.

Focus areas:

Think about the areas that require regular risk assessments. Be clear on what information you would like staff to check and design a series of forms to work for different risk areas. Set data governance rules to ensure data is captured in the format desired that will feed into your reporting process. Implement data governance to avoid blank fields and badly formatted, poor quality data. Consider automating the process using technology ensuring risk assessments are automatically sent out on a regular basis with limited work required from the risk team. If you can, adopt a process where data from risk assessment forms feeds directly into your risk management programme – avoiding manual data transfers that can produce errors.

5

Define a Risk Appetite and Operate Within It

Every organisation must absorb a certain degree of risk to run its operations, so defining a risk appetite is an important step for any business. For example; accepting that 5% of your stock might be lost through theft might seem tolerable, but 10% may not and you will want to spend money to implement further controls to reduce the risk. A risk appetite helps an organisation to decide where it would like to allocate budget or resources to implement policies, controls, and guidelines to reduce the risk.

A risk appetite is more than just a 'risk appetite statement'. It is about understanding your current risk levels and deciding if that is acceptable to the organisation. Risk will then be monitored on an ongoing basis - risks that exceed the threshold can be quickly flagged and addressed.

Focus areas:

Work on understanding your current risk exposure in each area and understanding the impact that each area has on operations and strategic goals. You can't set a risk appetite without knowing your current risk levels. Think about how you will measure the impact of the risk. Some risks may happen, but there may be no negative outcome, therefore you can adjust your acceptable risk tolerance accordingly. Consider industry standards and regulations when defining a risk appetite as there maybe certain risk factors that must be mitigated for regulatory purposes. Consider how risks in different areas of the organisation may impact each other and account for these interdependencies.

Make sure your risk appetite is documented and clearly communicated. Ensure the relevant stakeholders understand what is acceptable and integrate 'risk appetite' into the organisation's decision-making processes. If your risk levels are too high, focus on your current controls and test them to make sure they are effective, if they are not reducing the risk in line with risk appetite, the organisation may want to implement further controls or introduce policies and procedures to reduce the risk further. This is where risk management can truly drive decision making regarding budget & resources.

6

Establish Effective Controls

Having effective controls in place to reduce unwanted risk is an essential part of any risk management programme. Many of the risks on an organisational risk register could likely have a negative impact on the company, therefore it is important to establish effective controls to reduce each risk.

Controls can come in a variety of formats. A control could be a policy or procedure or some regular training that is implemented to make sure things are done in a certain way to reduce risk, it could be a regular check that takes place, or it could be spending budget on new systems, equipment, and security features to reduce risk.

When it comes to highly regulated sectors like financial services, 'controls' are often automated checks performed on large data sets to look out for unusual activity like high value transfers, overseas activity, or duplicate figures. These controls are often mandatory requirements and organisations must provide proof of adequate internal controls to regulators.

The type of control required will vary depending on the risk you are trying to control. Controls should be tested regularly to ensure their effectiveness, enabling organisations to implement procedures & further measures to boost control effectiveness in weak areas.

Focus areas:

Examine your risk register closely and think about the types of controls that would lower or reduce the impact of each risk. Remember a 'control' might be a policy or procedure that needs to be followed, it might be regular checks, it might be rules that are automated to perform checks in large operational data sets, or it might be a new system or piece of equipment to reduce the risk.

Whatever your controls are, be sure to assess them and check them regularly for gaps and vulnerabilities. Remember one risk can have multiple controls and a particular control can contribute to reducing multiple risks. Therefore, remember to ensure your risk management process allows for the complex mapping between risks and controls to ensure you can run reports to understand risk factors and the correlating control effectiveness.

7

Implement Effective Risk Response

Having effective controls in place to reduce unwanted risk is an essential part of any risk management programme. Many of the risks on an organisational risk register could likely have a negative impact on the company, therefore it is important to establish effective controls to reduce each risk.

Having a clearly defined escalation process is essential to keep risk at a tolerable level. Risk owners and escalation routes should be clearly defined. Many companies use the automated workflows available in GRC platforms to send automated notifications to relevant employees. Once a risk is escalated you must define what should happen – Who should check the control to see if it failed? What mitigating actions need to be taken? Do new policies, procedures, or controls need to be set up? Who needs to be notified? Having this defined up front and built into you r process framework will ensure prompt escalation and resolution of risk.

Focus areas:

Assess your risk register and define clear risk owners and escalation routes. Consider which teams might be affected by the risk and work out who should be notified if the risk is high. Define a clear process to capture the steps that were taken to resolve the risk, be sure to capture actions and timelines. Log the details around additional risk assessments and new controls & measures that were implemented. For each risk there are usually 4 risk response strategies:

- **Avoidance:** Eliminate the risk by changing plans or avoiding certain activities.
- **Mitigation:** Implement measures to reduce the likelihood or impact of the risk.
- **Transfer:** Shift the risk to a third party, such as through insurance or outsourcing.
- **Acceptance:** Acknowledge the risk without taking specific action, especially when the risk is within acceptable tolerance levels.

You should consider which option is best and define a clear process for each option.

No risk review or response process should be ad-hoc or left to chance. Learnings from each review and response cycle should be documented and mapped back to the risk review and response process. Organisations who take a reactive approach to risk tend to pull employees away from their day jobs to respond to a risk incident and then resume business as usual. A planned, systematic approach provides an organisation with the opportunity to stay ahead of risk incidents, rather than reacting when it is too late.

8

Comprehensive Risk Reporting

Being able to view instant reports on risk across different departments & sites can prove invaluable for an organisation. Capturing, tracking, and responding to risk events can be rapidly enhanced by using GRC software to convert risk information from a risk register into an array of dashboards & reports to understand risk exposure in real time. Dashboards can be customised to suit a range of roles & responsibilities. Front line staff can get a simple view of their outstanding risk related actions & tasks regarding data entry, control checks, and risk assessment completion. Managers & executives can get fast oversight and a single source of truth for analysing and tracking important risk data.

The instant reports available in GRC software enable stakeholders across the organisation to make informed decisions about how to best respond to risk incidents. Risk incidents can be captured and analysed together with the risk assessment and rating to provide insights into the effectiveness of current controls and treatment actions.

Most GRC platforms offer a wide range of risk reporting to summarise the entire risk register and give a high level view of the organisations risk landscape. Employees can drill down into problem areas to assess the detail. Other useful reports include heatmaps to visualise areas of high medium and low risk, bow-tie analysis to visually represent & analyse the potential causes, consequences, and preventive measures associated with a specific risk, and a whole host of KRI reports. Some solutions even offer executive level dashboards for external staff and board members who don't use their risk management tool but need to see live updates on specific areas.

Focus areas:

Decide on which data you need to track 'Key Risk Indicators' and work out how data will be captured and collected – whether that from from existing systems & data sources or through a series of risk assessments, checks, and data entry points. Once data is captured, establish who needs to see what information, and in which format.

Select a GRC platform that offers out-of-the-box reports that can easily be customised to meet any bespoke requirements - without coding or professional services fees. Look for reporting capabilities like KRI reports, heatmaps, and bow tie analysis to provide in depth insights into your risk profile.

Being able to view instant reports on risk across different departments & sites can prove invaluable for an organisation, that is why centralised risk reporting & oversight is a necessity when it comes to risk management.

Risk Management Adds Value

Risk management is so much more than simply ticking the 'compliance' box, it adds organisational value, and safeguards the organisation from potential threats, downtime, and loss of revenue. Successful organisations place positive value on risk management at a leadership level.

In modern progressive organisations, risk management is not seen as a problematic, arduous process with negative connotations. Nor is it a box ticking exercise to meet an external requirement. Instead, it is seen as a chance to pursue new opportunities, improve existing processes, mitigate intolerable risk, and drive positive business change overall. Organisations who opt to purely mitigate & reduce risk are likely to miss out on opportunities where they could 'take risk' that could bring a long-term positive outcome.

To ensure you and your team get the most out of your risk management process, make time to review audit outputs, risk registers, and dashboards. Conduct interviews and deep dives into problem risk areas, use the data to identify areas of opportunity, process improvement or efficiency, and use risk data to allocate budget for controls & mitigating actions, and for informed decision-making.

Be sure to ask operational leaders if the audit data reflects reality on the ground. Engage employees on whether company processes are supporting or hindering them. Be mindful, if company culture expects perfect documentation and clean audit trails, you might get exactly that. Clean audits every time might signal perfect risk management, or it might just mean employees are trying to keep the numbers in the green and are not taking active steps to reduce risk & improve processes.

To ensure you and your team get the most out of your risk management process, make time to review audit outputs, risk registers, and dashboards.

Taking Your Risk Management Programme to the Next Level

Most businesses need to absorb a certain degree of risk to achieve their strategic goals & objectives – which is why aligning risk management with strategic planning is a logical next step for ambitious organisations.

Risk management functions operating in isolation, in silos or as back-office functions can quickly become disconnected from business reality. Managers, executives, and key stakeholders need regular visibility and reporting on risk events and incidents in the context of their organisation's strategic and operational plans to guide decision making. Aligning risk to strategic goals and operational priorities also helps define relative risk importance.

Modern GRC platforms offer strategic planning capabilities that integrate with risk management. This allows an organisation to break down their strategy into a series of smaller programmes, tasks and actions and allocate them across the organisation with clear timelines and budgets. Any risks to achieving the strategy can be logged in the risk register and assessed and monitored as part of the wider risk management programme and the relevant controls can be implemented. This helps an organisation to mitigate any strategic risks that could derail their strategic plans.

Understanding the impact of risk on both strategic plans and overall enterprise performance is vital. A company may be spending large budgets to control a risk, but if the risk actually happened, and there was no impact to business operations, the spend on that control could be reduced. Similarly, if a risk level is seriously impacting performance and revenue, then an organisation will want to look at implementing new controls to lower the risk.

Focus on understanding how risk metrics link to strategic business priorities to take your risk management programme to the next level.

Focus on understanding how risk metrics link to strategic business priorities to take your risk management programme to the next level. Communicate risk metrics to senior stakeholders so they begin to consider risk as part of their strategic decision making. Design meaningful metrics & dashboards for decision-makers. This enables them to both consider the risk implications of their actions and make informed choices proactively in a strategic context.

Discover How Camms Can Streamline & Automate Your Risk Management Programme

The Camms platform offers full enterprise risk management capabilities. Set up a digital risk register, set KRIs, carry out online risk assessments, implement controls & corrective actions and view your risk data through a series of insightful dashboards & reports. Whether you are at the early stage of risk management or looking to advance you programme, request a demo of the Camms platform to discover how it can streamline & automate your risk management processes.

Camms.

www.cammsgroup.com

For more information

Visit Website

Request Demo