Camms.

Software to Change Tomorrow.

From Data to Decisions:
Engaging Everyone in Enterprise Risk Management for Business Success

ERM

Intro

Risk lurks in every area of your organisation across every team, department, and site. Risk is so widespread that it would be impossible for a small risk team to have visibility of every risk and manage it effectively - which is why an enterprise-wide approach to risk management is essential.

It is important to remember that while staff of all levels can cause unwanted risk to your business, they also hold the power to anticipate and prevent risk to safeguard your organisation.

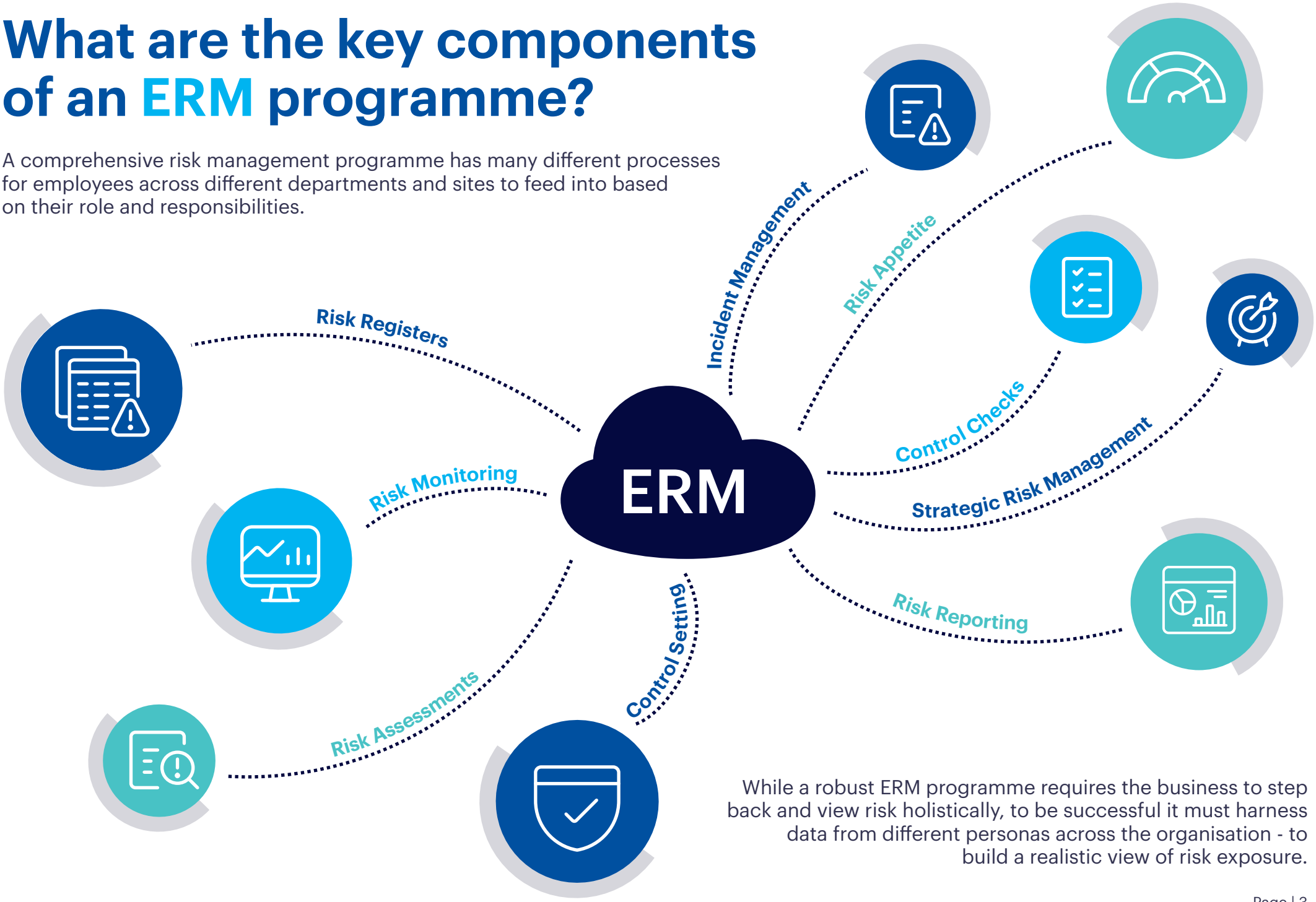
In this eBook we explain how to enable your entire organisation to feed into your Enterprise Risk Management (ERM) programme - providing more visibility of risk than ever before. We'll explain how everyone should be engaged in the risk management process from front line staff logging incidents and completing risk assessments & control checks right through to risk professionals, senior managers, and board members – who should be using risk data to inform decisions.

We will detail how each persona within your organisation should be involved in the ERM process to create an integrated approach to managing risk that aligns with your strategic objectives.

We will also share how the latest GRC software can provide a framework for a best-practice ERM programme and fully integrate and automate the process - eliminating silos and generating invaluable data to guide the organisation.

What are the key components of an ERM programme?

A comprehensive risk management programme has many different processes for employees across different departments and sites to feed into based on their role and responsibilities.



While a robust ERM programme requires the business to step back and view risk holistically, to be successful it must harness data from different personas across the organisation - to build a realistic view of risk exposure.

Risk Registers

Organisations should build comprehensive risk registers and categorise and rate risks according to their type and severity. For truly enterprise-wide risk management, firms must consider multiple risk areas including, operational risk, strategic risk, compliance risk, third-party risk, cyber risk and project risk. Once risk registers are established, risk teams must define Key Risk Indicators (KRIs) for each risk. In most organisations only certain employees will have the authority to log a risk & there will likely be an approval process to ensure it is categorised and rated correctly and is assigned the correct escalation route.

Risk Monitoring

Based on predefined KRIs, firms must decide how they will monitor the level of each risk – this will likely be based on a series of different factors including, risk assessment results, regular checks, operational data, number of incidents reported, questionnaires, and staff surveys.

Risk Assessments

Risk assessments are a fundamental part of any enterprise risk management programme. These are essential to understand levels of risk exposure and results should be captured centrally and analysed. Risk assessments are usually rolled out on a regular basis using a variety of forms that enable employees to answer questions regarding risk exposure. Most companies have a variety of different forms in circulation depending on the risk type.

Control Setting

Most risks on the risk register will likely have a control to reduce the risk level. Controls come in many forms including policies, procedure documents, regular checks, new technology or safety equipment.

Risk Appetite

Most organisations will work within a clearly defined risk appetite. Organisations will need to understand their current risk exposure and set tolerances to ensure they don't exceed the agreed levels. As part of an ERM programme, risk appetite will need to be linked to KRIs, risk monitoring and risk assessment results – enabling companies to ensure they are operating within their desired risk appetite and avoiding unnecessary risk.

Incident Management

Risks often turn into full blown incidents and many 'incident causes' are added to the risk register to prevent reoccurrence. Therefore, it is vital that incident reporting is factored into the risk management process. All employees should be able to log incidents and there should be clear routes for escalation and cases should be carefully managed until closed and resolved. Incidents should be able to be mapped to the relevant risk and vice versa.

Control Checks

Once an organisation has established a series of 'controls', they must perform regular control checks to make sure their controls are effective. This will help the organisation to establish if the current equipment, policy, or procedure is reducing the risk to a tolerable level or if they need to take further action to reduce the risk.

Strategic Risk Management

Not all risks are bad. An organisation needs to be able to understand which risks are worth taking to achieve their strategic goals, and which risks should be avoided at all costs as they will have a detrimental impact on their strategy. Uncovering these strategic opportunities for investment & growth and balancing risk vs reward involves scenario testing to understand the likely outcome of risk-based decisions and relies heavily on having sufficient risk data.

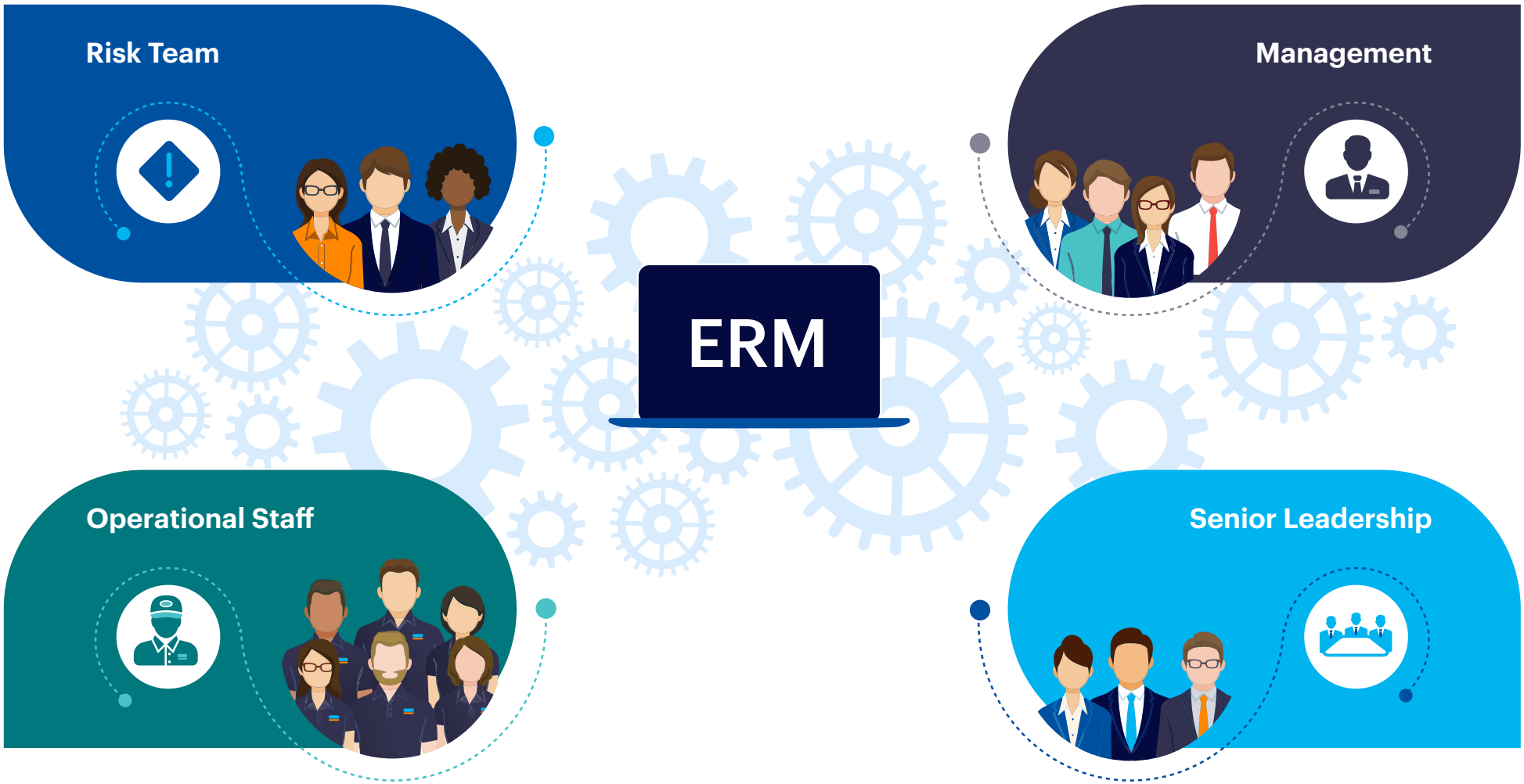
Risk Reporting

A huge part of any risk management programme is risk reporting. Managers and department heads need to understand risk exposure in their specific areas and risk teams and board members need to be able to report on risk to guide business decisions.

When we consider all these different aspects of ERM there is no way that one risk team can perform all of these different tasks across multiple teams, departments and sites throughout the globe. Therefore, it is important for any senior risk professional and their team to collaborate with different departments and sites to factor 'risk management' related tasks into their roles & responsibilities. Whether it be completing regular risk assessments and control checks or using risk data to make decisions, staff of all levels will need to engage in ERM as part of daily operations.

Persona-Led Enterprise Risk Management

Let's explore some of the different roles and responsibilities within an organisation and consider the important part they play in building a comprehensive approach to enterprise risk management.



Risk Team

Ultimately any ERM programme will be driven by the risk management team – often including a Chief Risk Officer and a team of risk professionals. These are the individuals that will likely be building the risk register, defining the risk appetite (in conjunction with the board), creating risk assessment forms, defining a framework to categorise & rate risk, and doing most of the risk related reporting. These risk professionals are responsible for embedding a risk-aware culture across an organisation and driving meaningful behavioural change.

The risk team will start out by building a risk register. Key risks will be added, and they should be categorised by type, likelihood, and severity. Key Risk Indicators (KRIs) will be set for each risk enabling them to know when risk has reached an intolerable level so action can be taken. Each risk should be allocated an owner, and a clear escalation route should be defined so the correct individuals are notified when the level of risk is too high.

To support with risk monitoring efforts risk teams will also need to design a series of risk assessment forms that can be rolled out on a regular basis to continually monitor risk exposure. Forms will likely vary depending on the type of risk. Risk teams will be responsible for rolling out these assessments, capturing the results and ultimately analysing the findings.

Risk teams will also be responsible for working with the board to define the organisations 'risk appetite'. They will have to provide a complete overview of the organisations current risk exposure and work with the board to understand what level of risk can be tolerated and what level of risk is deemed 'too high'. This will enable them to work with the organisation to implement additional controls to reduce risk.

To a certain extent, risk teams will also be involved in control setting and control checks, although they will not necessarily implement the control or perform the regular checks, they will be responsible for managing the control register and for ensuring checks are carried out on a regular basis.

Risk teams are also likely to be involved in setting up an organisation's incident management process. It is often the risk team's responsibility to create an incident register and define a process for employees to report incidents. Incident logs are a great source of risk management data as they contain a wealth of information about incidents, hazards and near-misses which should feed into the wider risk management programme.

Finally, it is the risk teams who will need to run the majority of the reports to understand risk exposure and advise the business on the best course of action. When defining any ERM programme, it is important for the risk team to consider what reports they will need to run for themselves and the wider organisation. This will ensure the relevant data can be collected to feed into the desired reports.

Operational Staff

The biggest segment of an organisation's workforce are often the operational frontline workers. These individuals are the feet on the ground often witnessing risky situations, hazards, and incidents as they happen. Therefore, these individuals are often an organisations' biggest and most trusted source of risk data. The breadth of their usage makes them the most important users in terms of implementing organisational change, despite only having limited responsibilities and not typically being trained in the theory of GRC. The challenge for risk professionals is to engage with these individuals and harness their potential to act as a catalyst for meaningful change.

Front line workers will be the individuals who are responsible for completing risk assessments. Risk assessment forms will need to be filled out on a regular basis to monitor risk levels. This data should be simple to complete and should be positioned as part of the employee's role.

Frontline workers will also likely be the individuals feeding into the incident management programme - logging incidents, hazards, and near-misses. They should be able to log incidents as and when they happen – capturing critical data regarding, date, time, employees involved, location, and any photos and evidence of the incident.

Front line workers will also be those performing regular control checks and control testing. Whether it is ensuring employees are operating in line with policies & procedures or ensuring equipment is working or carrying out a series of regular checks – these front-line workers are the key to understanding if your controls are effective. Control checks should be carried out as part of their daily roles and responsibilities.

To get the relevant data from these teams, it is important to provide training on how to enter the data and implement measures to ensure data is entered in the desired time frame and format.

Risk reporting is not necessarily relevant for these employees, but it is important that they can get a simple view of their outstanding tasks and actions - enabling them to complete the relevant data on time. Having front line employees actively feeding into the risk management programme will build a risk aware accountable culture where employees feel responsible for risk in their own area.

Management

It is important for risk teams to establish ‘risk champions’ throughout the business. These stakeholders are assigned individual responsibility for certain risks and controls throughout the organisation. They are often ‘team leaders’ or ‘departmental heads’ or ‘managers’ who have more of a direct responsibility for certain risk areas as part of their role.

As these individuals have a more senior position, they will not necessarily be completing risk assessments or control checks. They will be analysing the data from completed risk assessments and control checks and addressing any problem areas.

These risk owners will likely be the individuals notified if a risk level is deemed too high or a control was failing. They will have the authority to make a decision regarding whether they accept the risk, mitigate it with a control, transfer it, or change plans to avoid it completely.

Control owners will have responsibility for making sure the relevant control is implemented and is effective and they will likely have the authority to suggest new controls and policies that can be added to the control library and managed as part of the wider ERM programme.

They will still have the ability to report any incidents, hazards and near misses as a standard employee, but they may also be responsible for resolving certain incidents in their areas and will likely be part of the incident escalation process.

Reporting will also be fundamental for these risk and control owners. They will need to be able to summarise the results of risk assessments and control checks to understand risk exposure in their specific area so they can address potential problems. They will also need to view reports on ‘controls’ and ‘control effectiveness’ as they may want to introduce additional measures in areas where risk levels are on the rise.

Senior Leadership

Business leaders like directors and board members are not typically risk professionals, but to fulfil their role, they must understand risk data, and leverage the resulting information to make informed decisions. Companies do not have an infinite budget to control and mitigate all risks. Therefore, these leaders will want to get a holistic understanding of risk exposure and potential consequences throughout the organisation so they can decide where to allocate budget and resources – in order to reduce the most critical risks.

These high-flying executives won't be interested in individual risk assessments and control checks they will want to view an amalgamated data set summarising risk levels across the entire organisation with the ability to drill down into problem areas so they can be addressed.

These individuals will still likely need the ability to report any incidents, hazards and near misses as part of the wider incident reporting process, but ultimately their focus will be on using risk data to make important decisions regarding budget allocation, resourcing, and organisational strategy.

For these stakeholders it will also be vital to understand risk in the context of the organisation's goals and strategic objectives. They may want to take risk in a certain area if it will likely help them to achieve their strategy. Or there might be particular risks that could have a detrimental impact on their strategy that they will want to avoid at all costs. Mapping risk to key goals and organisational objectives has proved to be fundamental to keep an organisations strategy on track.

Generating the right risk reports is key for senior leaders. They rely on accurate data to make critical decisions regarding budget and resource allocation affecting multiple departments. Incorrect risk data could result in poor decision making - resulting in costly errors.

What are the problems with manual spreadsheet-based ERM?

Some organisations are still using spreadsheets to manage risk. And while it can be a good place to start for some smaller businesses, as organisations expand, it becomes unmanageable. Complex processes like ERM require multiple users, complex data mapping, control monitoring, automation, strict data governance, and in-depth reporting & analytics – and spreadsheets simply don't offer this level of functionality.

Here are just some of the problems with manual spreadsheet-based ERM programmes:

- Poor quality risk data due to a lack of data governance.
- Duplication of effort and increased admin as data often needs to be transferred between forms and various spreadsheets.
- Spreadsheets don't integrate, making it hard to get a consolidated view of risk.
- No standardised risk framework, making it hard to prioritise the most critical risks.
- Access issues resulting from multiple employees trying to amend the same spreadsheets – often resulting in over written data.
- A lack of accountability – making it hard to know who amended what and when.
- Difficulty mapping risk to the relevant controls and associated incidents across multiple spreadsheets.
- A lack of automation means all risk assessments are sent and chased up manually, data is transferred by hand, and there are no automated notifications and alerts to flag problems or workflows to formalise processes.
- Time consuming and cumbersome reporting that only gives a moment in time snapshot of events.
- No formal links between risk and organisational strategy making it hard for organisations to take the right risks to achieve their strategic goals & objectives and improve performance.

How does GRC technology make it easy for every employee to feed into the risk management programme?

GRC technology provides a simple online platform that allows employees of all levels to feed data into the ERM programme as part of their daily role, building a risk aware accountable culture. These platforms make it easy to collect risk data from across the organisation using simple online forms that feed directly into the platform. These tools contain all the functionality needed to build a comprehensive risk register and a best-practice risk framework. They offer automated workflows to streamline and automate the entire risk management process and they offer a wide variety of dashboards & reports to visualise risk data.

Let's delve into each aspect of the ERM process and discover how GRC technology can simplify and automate the process. We'll also share insights into how each persona would use the GRC tool to carry out their risk related tasks.

Building a Risk Register

Organisations would build a digital online risk register directly within the GRC platform, this would usually be initiated by the risk team in conjunction with key stakeholders. The clean, interactive, and searchable risk register can be easily filtered and accessed online by multiple employees at once. Hierarchies can be set up to ensure employees only see the information relevant to them – so they are not overwhelmed by vast amounts of data.

Predetermined templates are available to log risks, and these can be customised to include any additional information that needs to be captured. User permissions ensure only authorised employees have the authority to log a risk and predefined approval workflows ensure risks are verified quickly so they can be effectively managed. Data governance rules in the form of standardised fields, menus, and drop-downs ensure risks are logged accurately and consistently – resulting in accurate reporting outputs.

Key risk indicators (KRIs) are then set for each risk, and risks can be allocated to the relevant owner via integrations with an organisations 'active directory'. Organisations will also have to decide how they will monitor the risk level of that risk and determine what data they will need to understand the current status of that risk. Operational data can easily be pulled into the platform from other systems and data sources via API integrations, making it easy to get a consolidated view of risk exposure in certain operational areas. Results of any online risk assessments, checks, questionnaires, and surveys also feed directly into the platform to provide further insight into risk levels.

Best-practice risk frameworks make it easy to categorise and rate each risk consistently across the organisation according to its type & severity - making it easy to compare risk across the entire enterprise. Organisations can have unlimited risk registers, categories and types and run reports and view dashboards to drill down into specific risk areas.

Daily tasks would include:

Risk Team

- Adding or approving risks to go onto the risk register.
- Viewing risk register summary reports and actioning the findings.

Operational Staff

- No visibility of the full risk register required.

Management

- Adding or approving risks to go on the risk register.
- Viewing risk register summary reports for their own area.

Senior Leadership

- Viewing high level risk register summaries.

Risk Assessments

When using a GRC platform all risk assessments are carried out via online forms with all data feeding directly into the platform. The best-practice online risk assessment forms contain the recommended fields for a robust risk assessment – and firms can further customise them based on any individual requirements. Different forms can be established for each risk type - ensuring forms include the relevant fields to capture sufficient data. These platforms also enable staff to upload, photos, documents, and voice recordings as part of a risk assessment to fully document the risk.

The circulation of risk assessment forms and any necessary chasing for outstanding actions can also be automated by the GRC platform. Risk teams simply build a schedule of the required risk assessments, and the platform sends an email notification to the employee responsible for carrying out the risk assessment. They can click on a link in the email and complete the form online. If the risk assessment is not completed by the due date, the automated workflows in the system will automatically send reminders and escalate where necessary.

Most GRC platforms offer a mobile app - allowing teams to complete risk assessments, actions, and tasks on their phone or tablet. This makes it quick and simple for staff to complete assessments anytime, anywhere even without Wi-Fi – data is uploaded when a connection is re-established.

As staff are completing risk assessments and checks, the platform keeps a full record of who entered what, and when the data was logged. This enhances accountability and ownership for risk. The data governance guidelines & automation ensure fast, accurate, timely risk assessment data that links to any associated risks on the risk register, providing an instant view of risk levels.

Daily tasks would include:

Risk Team

- Scheduling risk assessments.
- Analysing the results of completed risk assessments.

Operational Staff

- Completing risk assessments.

Management

- Completing risk assessments.
- Receiving notifications of problematic risk assessments for their area.

Senior Leadership

- Viewing a summary of risk assessment results to identify problems areas that need investment.

Risk Monitoring

GRC platforms simplify risk monitoring efforts substantially by automating the process. When risks are added to the risk register, risk teams will decide in collaboration with stakeholders across the business how the risk level will be measured, what the KRIs will be, and what metrics deem that the risk is too high, and action must be taken.

Risk levels are usually monitored based on the results of risk assessments, checks, questionnaires, surveys, incident levels, or by using operational data from other platforms and data sources. A GRC platform makes it easy to consolidate all that data. The results of online risk assessments, surveys, and checks all feed directly into the platform and are automatically linked to the corresponding risks. Any operational data that could provide insights into risk levels can also be fed into the platform via API integrations with other systems and spreadsheets – making it simple for firms to consolidate all their vital risk monitoring data in one central platform – ensuring a single source of truth.

Rules can be set within the platform to notify the relevant stake holders when risk levels are too high so they can make important decisions about whether to accept the risk, mitigate it with a control, transfer it, or change plans to avoid it completely. These instant risk notifications and defined escalation routes enable firms to address risk quickly and keep operations within their agreed tolerance levels.

Risk teams, managers and leaders can view instant dashboards & reports to understand risk exposure in specific risk areas without any data manipulation – enabling them to easily understand problems.

Daily tasks would include:

Risk Team

- Viewing risk levels and advising leaders on the best course of action.

Operational Staff

- Performing regular checks to monitor risk levels.

Management

- Receiving notifications of high-risk areas so they can address them.

Senior Leadership

- Viewing high level reports on risk exposure.

Control Setting

Firms can build a complete digital library of all their controls within the GRC platform. Controls are entered using simple online forms that can be configured by risk teams to ensure the relevant data is captured. Typically, firms capture details regarding control owner, category, type, associated regulations & policies, testing method & frequency, control changes, and current status.

Whether the control is a policy or procedure, a step-by-step process, regular training, safety equipment, technology or software related e.g. firewalls, encryptions, access controls, or security related e.g. cameras, guards, alarms, and barriers - it can all be captured in the platform.

The data enables risk teams to understand control effectiveness enabling them to suggest further controls in areas where the risk is increasingly high.

Most GRC platforms can integrate with an organisations active directory allowing them to easily assign control owners. The integrated nature of GRC platforms allows firms to easily map controls to the associated risks. Controls can be linked to multiple risks to build visibility of risk levels.

Daily tasks would include:

Risk Team

- Adding controls to the control register.
- Monitoring of control effectiveness.

Operational Staff

- No involvement in the control register.

Management

- Adding or approving controls to be added to the risk register.

Senior Leadership

- Viewing high level summary of current controls & their effectiveness.

Control Testing

The process of control testing can also be simplified using a GRC platform. Once the control register is built, regular dates can easily be scheduled for testing activities. Testing schedules can be set up to ensure that controls are regularly assessed according to regulatory requirements, organisational policies, or industry standards.

When a control test is due, an email notification is sent to the relevant employee to make the necessary checks. Control checks involve various activities such as reviewing documentation, conducting interviews, observing processes, or performing transaction testing. GRC platforms often provide tools to facilitate testing activities, such as checklists, templates, and workflows. The results of each individual test are entered directly into the platform by the employee via an online form, this includes recording observations, findings, and any deficiencies or issues identified during the testing process. Test results may also include evidence or supporting documentation to validate the effectiveness of controls.

The GRC platform automatically sends out notifications to chase up any missed or delayed testing activities – ensuring prompt timely information. If control deficiencies are detected, GRC platforms facilitate the tracking and management of remediation activities, including assigning tasks, setting deadlines, and monitoring progress towards resolution.

GRC platforms offer reporting and analytics capabilities to summarise control testing results. Reports often include dashboards, scorecards, trend analysis, and regulatory compliance summaries to support decision-making and risk management efforts.

Daily tasks would include:

Risk Team

- Scheduling control checks.
- Analysing the results of completed control checks.

Operational Staff

- Carrying out control checks.

Management

- Approving or overseeing control checks and ensuring their completion.

Senior Leadership

- Viewing high level summary of current control effectiveness.

Incident Management

GRC software makes it easy for firms to set up a best-practice incident reporting process as part of their wider ERM programme. Risk teams define how they will categorise and rate incidents and how they will be escalated – this forms a framework for the incident management process.

From there, employees can easily go into the platform and log any incidents, hazards, or near-misses that they witness using online forms – with all data feeding directly into the tool. Businesses can create multiple form layouts for different categories and types of incidents. Common categories include, cyberattacks, data breaches, system failures, physical incidents & accidents, employee misconduct, customer complaints, and compliance violations. Data governance – in the form of menus, drop-downs, and auto-formatting - ensures all relevant data is captured in a consistent format. Employees can also upload photos, URLs, and documents into the tool to provide critical evidence of each incident logged.

Once captured, incidents are then rated on their criticality & type and escalated accordingly. Automated workflows escalate the incident to the relevant stakeholder based on its type and severity. Out-of-the-box investigation templates expedite the process allowing for prompt resolution of incidents. Workflows are also used to triage incidents, conduct root-cause analysis, and resolve incidents until cases are closed.

The software keeps a complete record of every incident logged and how it was escalated and ultimately resolved. This makes it easy for firms to understand where most incidents are occurring so they can implement preventative measures. Teams can run incident reports on certain incident types or business areas enabling different departments to address their individual problems. Firms can run reports on unresolved incidents and outstanding actions to expedite the remediation process.

Most GRC software platforms offer a mobile app enabling teams to report incidents on the move and complete outstanding incident related tasks and actions. Some GRC platforms offer external vendor portals - enabling third parties and contractors to log incidents online. This can also facilitate anonymous incident reporting for more sensitive matters like whistleblowing.

Daily tasks would include:

Risk Team

- Analysing the results of incidents logged.
- Understanding the relation between incidents logged and the associated risks and controls.

Operational Staff

- Logging incidents.

Management

- Logging incidents and supporting to resolve escalated incidents in their area.

Senior Leadership

- Viewing high level summary of incidents.

Risk Appetite

When it comes to GRC software, a risk appetite is so much more than a 'statement'. Companies can use the data and frameworks in the tool, to set rules relating to their risk appetite and receive alerts when the risk level is approaching or exceeding the agreed risk appetite.

Once a risk register is built, and Key Risk Indicators (KRIs) have been established, firms can agree their maximum risk tolerance and decide what steps should be taken and what controls should be implemented if the risk exceeds the agreed level.

Automation supports the risk appetite process as when the level of risk exceeds the agreed tolerance, automated notifications are sent to the relevant risk owner alerting them so they can take action. The platform captures remediating actions and continually monitors risk levels.

For risks that are continually exceeding their risk appetite, teams can implement new controls and perform regular control checks and control testing to further control the risk. All actions are documented ensuring organisations have an audit trail of events to meet risk management standards.

This automated functionality makes it simple for organisations to operate within their risk appetite and run reports on how they are performing in relation to their tolerated risk levels

Daily tasks would include:

Risk Team

- Working with stakeholders to define the risk appetite.
- Monitoring risk levels against the risk appetite.

Operational Staff

- No involvement.

Management

- Monitoring risk levels against the risk appetite in their area and addressing problem areas.

Senior Leadership

- Viewing high level summary of performance against risk appetite.

Risk Reporting

Risk reporting is an area where GRC software excels. The instant reports and live dashboards provide real time risk insights at the touch of a button – cutting back on manual data manipulation and reporting efforts.

Live dashboards enable each employee to get a 'quick view' of their risk related tasks and actions and a summary of key statistics. Each dashboard is personalised according to a staff members role & responsibility. Lower-level staff will see a summary of their upcoming tasks and actions relating to carrying out risk assessments and control checks, managers will see an overview of their notifications regarding risk escalations and approvals and a summary of the risk levels in their specific area, and risk professionals and leadership teams can view risk exposure across the entire enterprise and drill into specific areas. Senior leaders will also have a lens on how risk is impacting enterprise performance and strategic objectives.

Reporting is equally as impressive when managing risk in a GRC platform. Leaders and risk professionals can easily pull risk reports at the touch of a button. Most tools offer a variety of reporting options straight out-of-the-box and these can be further customised to meet any bespoke requirements.

Most solutions offer a variety of reporting outputs including risk register summary reports, control effectiveness reports, incident reports, KRI reports, heatmap reports to understand the likelihood and severity of risk types, and bow tie visualisations (to provide a clear representation of potential hazards, their causes, and the controls put in place to mitigate them). Many platforms even offer Microsoft Power BI interactive risk reports.

In most GRC platforms, users can build their own custom reports enabling them to easily summarise key data. This reporting automation eliminates the time risk teams spend on data manipulation and manual report building, leaving them more time to analyse risk reporting and use the data to guide the board about where best to allocate budget and resources to reduce risk.

Types of reports accessed would include:

Risk Team

- Full spectrum of risk reports including heatmaps, bow tie visualisations, summary reports, power BI reports, incident reports, and control effectiveness.

Operational Staff

- A dashboard of their personal upcoming tasks and actions.

Management

- Dashboards and reports on department and team risk exposure.

Senior Leadership

- Viewing high level summary reports of risk, controls and incidents across the entire enterprise.

Strategic Risk Management

GRC platforms can also support with strategic risk management as they enable firms to manage risk, plan & execute their strategy, and track enterprise performance in the same platform. This integrated approach enables firms to facilitate essential mapping and linkages between these areas enabling them to make important decisions about which risks are worth taking to improve performance and achieve their goals and which should be controlled and avoided as it will have a detrimental impact on their strategy and negatively impact performance.

Firms start by entering their top line strategic goals into the platform. These are then broken down into a series of smaller programmes, projects and tasks and allocated out across the business to different stakeholders for completion. Simple tree views help you visualise your plan as you build it. Everything is allocated a timeline, owner, and budget and fully planned out. As tasks are completed, progression is shown at every level of the strategy and notifications ensure timely completion of events and send reminders for overdue actions.

Risks and dependencies can be captured for each stage of the strategy and managed accordingly. This important mapping between risk and strategy enables organisations to manage strategic risk effectively and get full visibility of their risk exposure. A variety of reports and dashboards support organisations to demonstrate how operational initiatives are contributing to high-level organisational objectives and measure their impact. The reports enable firms to know whether their strategic plans are having the desired effect – empowering them to either demonstrate success or make the necessary alterations. Strategic risks are managed and controlled as part of the wider Enterprise Risk Management (ERM) programme.

Daily tasks would include:

Risk Team

- Viewing reports to understand the impact of risk on strategic objectives.

Operational Staff

- Logging the completion of small tasks that contribute to the overall strategy.

Management

- Viewing reports on strategic progress and strategic risk in their area and logging the completion of strategic tasks.

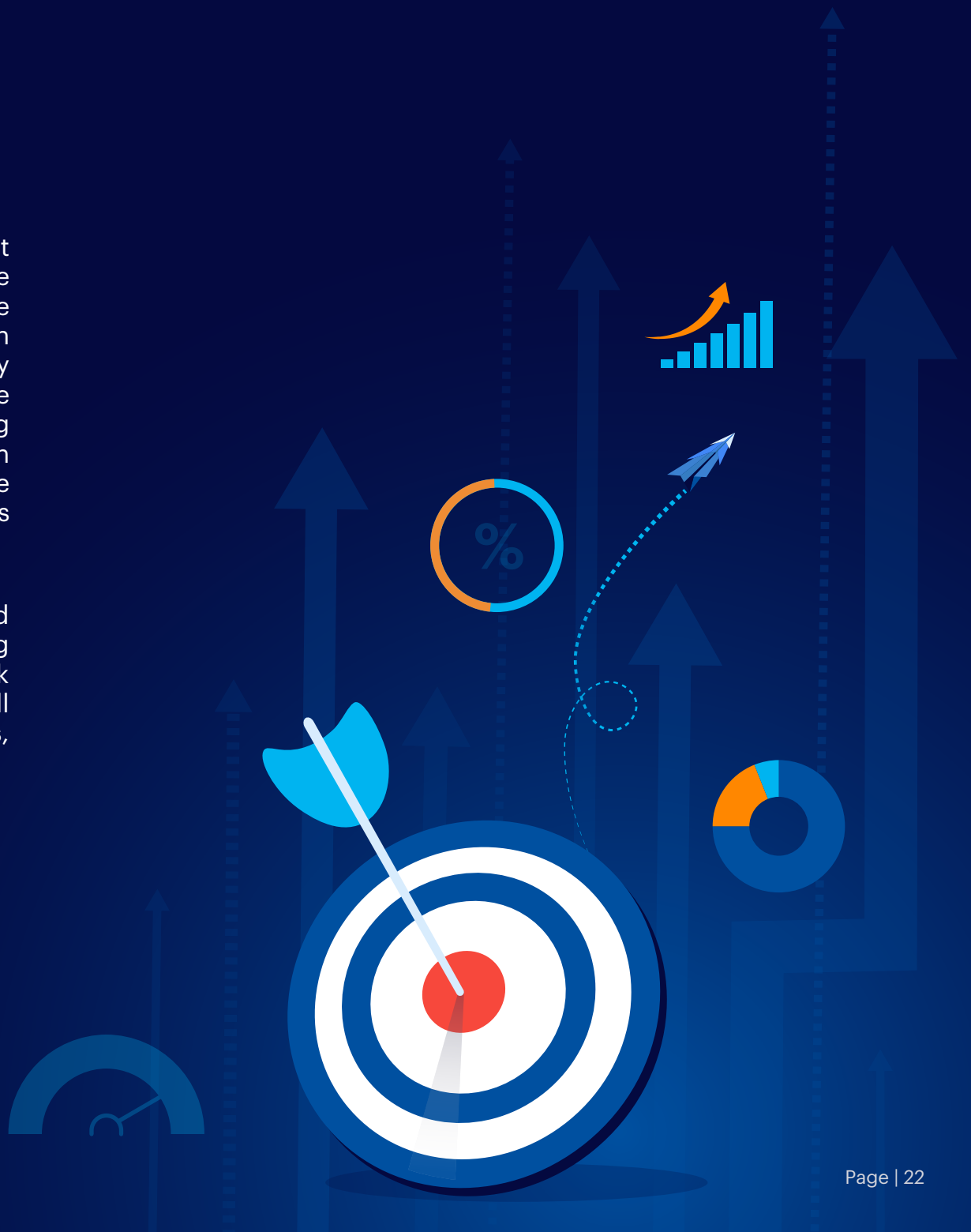
Senior Leadership

- Viewing a high level summary of strategy progression and enterprise risk exposure.

Managing risk in alignment with strategic objectives and enterprise performance

Of course, Enterprise Risk Management (ERM) is more than just managing different types of risk and enabling everyone in the organisation to feed into the risk management process. The primary objective of ERM is to ensure that the organisation achieves its strategic objectives without taking unnecessary risk. It involves integrating risk management into the organisation's overall strategic planning and decision-making processes - considering the interdependencies between different types of risks and their potential impact on the organisation's ability to achieve its objectives. This enables businesses to strike the right balance between risk and reward.

In a strong ERM programme, senior management and the board of directors should be involved in setting a risk appetite, making strategic risk decisions, and gaining oversight of the overall risk management process. ERM must consider the interests of all stakeholders, including shareholders, customers, employees, regulators, and other external parties.



How can ERM technology support my organisation to manage risk in line with strategic objectives?

Modern GRC solutions enable firms to plan and execute their strategy in the same platform as their ERM programme. This allows firms to map 'risk' to business performance and organisational objectives to understand its impact. This alignment lays the strategic foundations for an ERM programme to build organisational value by informing business decision-making and ensuring resources are allocated to the most critical risks.

Modern enterprise GRC platforms contain best-practice forms, templates, and workflows enabling businesses to fully map out their strategy and track progression. Firms will decide on their topline goals & objectives, and these are then broken down into smaller programmes, projects, tasks, and actions which are carefully planned out and allocated timelines, budget, and ownership. This approach ensures the entire business is accountable for achieving aspects of the strategic goals set by business leaders and allows individual stakeholders and teams to understand the part they play in achieving the overall strategy - ensuring the entire business is accountable for achieving the strategic goals set by business leaders.

Management can easily view the strategy map, and as tasks and actions are completed, progression is indicated at every level of the strategy. It's essential for leaders to get a clear view of how smaller tasks and projects are progressing and to understand how they impact the completion status of large strategic programmes.

As part of the setup, strategic risks will be captured as part of the wider ERM programme. Any risks that could negatively impact strategic goals & objectives or overall enterprise performance should be captured, monitored, and controlled to ensure strategic plans remain on track.

There may also be situations where the company needs to pivot and amend their strategy based on changes in the market and trading conditions. Managing strategic plans within an enterprise GRC platform makes it easy for management teams to make strategic changes –alterations are made in the platform, and automated workflows cascade the changes throughout the business – ensuring full transparency and accountability.

By linking risk management with the business strategy using an automated holistic platform that allows all stakeholders to feed data into both functions, the ERM programme becomes aligned with strategic goals and objectives. This comprehensive ERM data can then be leveraged to help run the business and create positive change, rather than focusing solely on mitigating operational risks and protecting the organisation.

Adopting an integrated approach to risk management and strategic planning provides leadership teams with an in-depth understanding of how different risks could impact strategic goals and objectives. This knowledge empowers leaders to develop more resilient risk-informed strategies that are focused on delivering performance results and enabling long-term viability.

Automated ERM: A Business Enabler

GRC solutions are essentially evolving into 'business platforms' that are used by employees at all levels to enter data as part of their daily role. This collection and subsequent aggregation of vital data - related to risk exposure and strategy progression via a centralised platform - fosters a holistic approach to risk management.

Empowered by this, small risk teams can capture data from across the business, set controls, and work with multiple teams, departments, and stakeholders throughout the enterprise. They can then focus their effort on analysing the risk data, understanding how it impacts the strategic plans, and advising the board on the best course of action - such as implementing controls in high-risk areas which will require budget and resources.

An intuitive GRC software platform can pave the way for multiple employees to feed data into the ERM programme and contribute to strategic progression because:

- Anyone in your active directory can own a risk, perform a control check, or complete risk assessment online.
- Staff at all levels can use the solution as part of their daily role, performing simple tasks like risk assessments and control checks via online forms, with all data captured fed into the risk programme.
- Leaders at different levels of the organisation can view risk linked to their specific area, and the board can get a holistic view of risk across the entire enterprise.
- Staff of all levels can own actions or tasks related to the overall strategy, and the completion of those tasks within the platform enables the board to easily understand strategic progression.
- GRC platforms offer a variety of different reports & dashboards – enabling firms to visualise their risk exposure and the impact of risk on enterprise performance and strategic plans.

As data analytics become more intricately linked with business decisions, the use of inaccurate data for risk management programmes can expose businesses to unforeseen risks, financial penalties, and reputational damage relating to non-compliance.

High-quality data entry is key, and GRC platforms make it simple for employees of all levels to enter timely accurate data thanks to a whole host of data entry rules and guidelines including, menus, dropdowns, auto formatting, mandatory fields, workflow automation, and step-by-step processes. Robust data governance generates high quality data that can be relied upon to make informed business decisions.

Modern ERM platforms are taking boardroom-based strategies and embedding them into business operations to ensure success – ensuring the associated strategic risks are managed along the way. ERM platform functionality is making it simple for organisations to map and link risk to enterprise performance and strategic objectives - to easily understand the correlation between the areas.

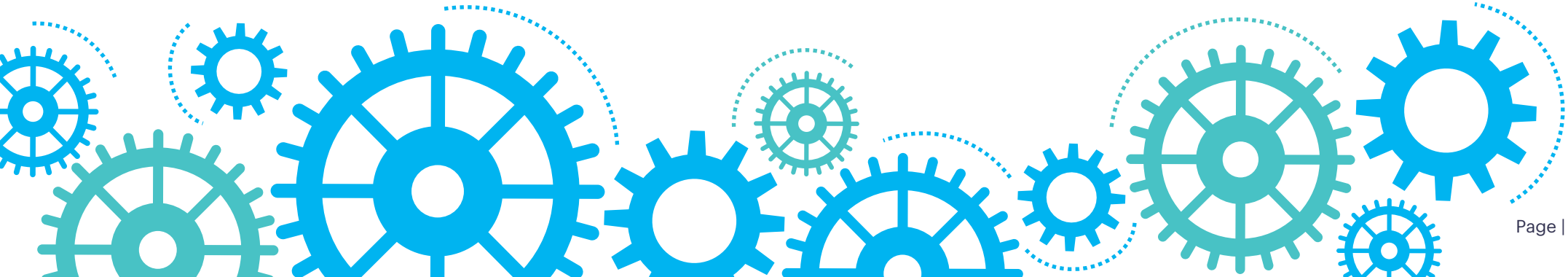
The intuitive interface means users can easily implement workflows for changes and approvals, ensuring processes are completed from start to finish with the proper authorisation. Automatic notifications can be sent when there are anomalies in the data, certain risk levels are reached, or actions require approval or completion.

Instant access to reports and dashboards allows users to view progress and provide updates for management, auditors, and regulators. When risk data is stored in a spreadsheet, it's just data; when it’s enriched by a GRC platform it provides valuable insights and informs decisions – adding value to the business.

Amid this liberation of data, risk management has become an organisation-wide discipline with personnel at all levels responsible for tasks or actions relating to aspects of risk and compliance, strategic objectives, and business performance – all captured in one holistic business system.

Empowered by the resulting information, risk management can be linked to strategic objectives, enabling business and risk leaders to understand which risks will negatively impact their strategy and which calculated risks they should take in pursuit of their objectives.

As GRC solutions transform into modern business platforms that are embedded more deeply within organisational processes – instead of disjointed systems adding disconnected layers of complexity – they’re breaking down siloes and supporting a coordinated approach to ERM that’s enhancing business resilience, agility, and performance.



About Camms.

Camms is one of the few ERM solutions that offers strategy planning in the same platform. This enables organisations to seamlessly align risk management with both strategic objectives and enterprise performance.

This single source of truth fosters a holistic ERM programme that can grow and evolve with the business, engage stakeholders, and optimise business performance by ensuring the organisation is taking the right level of risk to achieve its strategic goals and objectives – while successfully controlling and mitigating intolerable risk.

Core capabilities of the Camms platform include:

Risk management

Teams can set up a comprehensive risk register, track progress, and define KPIs and tolerances based on their risk appetite. Use the structured framework to define ownership and set key risk indicators, set automatic workflows & alerts to flag problems, and implement structured approval processes.

Strategy planning

Break down your strategic goals & objectives into lower-level projects & tasks and allocate them across the organisation to easily monitor performance and track progress.

Cyber and IT risk

Manage cyber and data privacy risk and ensure compliance with ISO standards and data privacy laws like GDPR. Monitor IT risk and track cyber related incidents.

Third-party risk

Set up a vendor register and monitor vendor risk. Roll out online vendor risk assessments and carry out benchmarking and scoring. Formalise supplier onboarding and off boarding and monitor performance against KPIs and SLAs.

Incident management

Facilitates incident and near miss reporting in real-time and triggers the investigation process post-event. Link incidents back to the originating risks.

Audit management

Schedule and manage internal and external audits and formalise the results and required actions. The solution provides a complete history of all your audits and their findings and any outstanding actions.

Stakeholder dashboarding

Intuitive functionality provides executives and the board with key risk, compliance, and strategic progress information when required.

Compliance

House a comprehensive obligations library of relevant regulations, legislation, policies, and internal procedures. Establish structured processes for version control, approvals, and regulatory change. The solution integrates with third-party regulatory content providers to offer regulatory horizon scanning.

Governance

Implement workflows, registers, and sign-off procedures for any process – including safety checks, feedback & complaints, disclosures, inspections, whistleblowing, questionnaires & surveys.

API integrations

Transfer data from other systems in and out of the Camms ERM solution via API connections, enabling you to base KPIs and risk monitoring on live data.

Analytics & reporting

Built-in dashboards and standard reports provide critical risk insights and executive reporting satisfies requirements from auditors & regulators.

Create an ERM programme that aligns with your strategic objectives

The Camms ERM platform has all the functionality you need to effectively manage enterprise risk and develop and execute your corporate strategy.

The platform offers best-practice forms, templates, registers, workflows, dashboards and reporting outputs to implement a comprehensive ERM programme that aligns with strategic objectives and enterprise performance goals. The intuitive user interface enables the entire organisation to feed into the ERM programme as part of their daily role.

Our team would love to learn about your ERM goals and strategic objectives and explore how technology can help you generate the right insights to achieve success.

Visit Website **Request Demo**

Camms.

Software to Change Tomorrow.