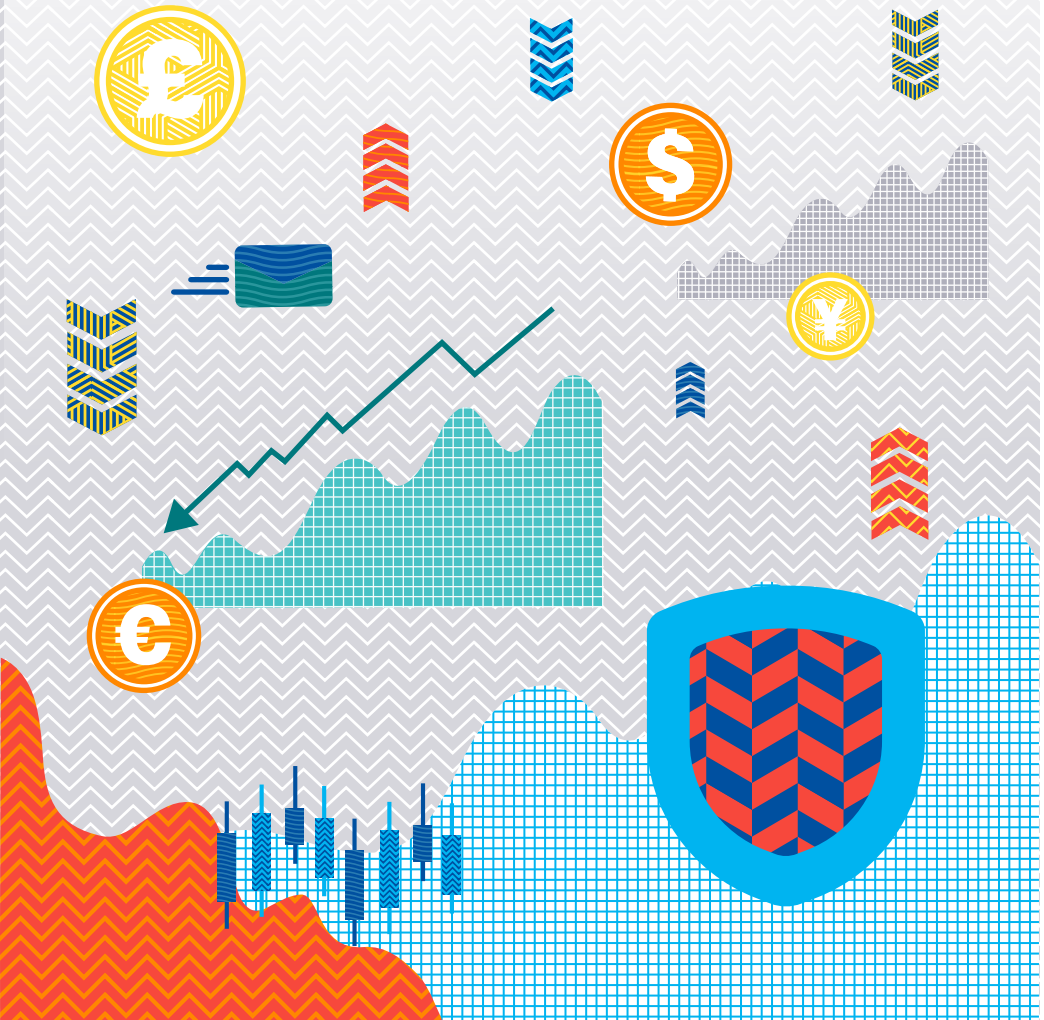
10 GRC Capabilities Financial Firms Can't Do Without!

Intro

Managing Governance, Risk, and Compliance (GRC) is a fundamental part of the operating model of any organisation in the financial services sector. Automation of risk and regulatory change management processes is nothing new for large top tier banks and financial services firms. What's changed is the pace at which the capabilities of these software solutions are evolving and the number of smaller, mid-tier players entering the market that are still using spreadsheets and legacy systems to manage this critical function.

In this eBook, we explore some of the capabilities that are taking GRC technology - and the financial services firms that leverage it - to the next level. Learn how multinational banks & large financial services organisations are evolving their GRC programmes by embracing new technology capabilities to generate business intelligence, improve their understanding of business operations, and create an agile business model. Plus, find out how smaller start-ups and challenger banks can leverage some of those tried and tested technology solutions to improve their own processes.

What are the key drivers behind this heavily regulated, high-risk sector?



Risks and regulations are inseparable bedfellows in the banking and financial services sector. This relationship was put to the test by the global financial meltdown in 2008-2009, prompting a period of re-regulation. As the sector emerged from this tumultuous period, governments and regulatory authorities were forced to implement a raft of new or stricter requirements amid an avalanche of risks.

This catalyst for seismic change transformed the banking and financial services sector into a highly regulated industry. Since then, other major events – such as the FinCEN files scandal and the COVID-19 pandemic – have reinforced the value of maintaining a robust and agile regulatory environment that insulates businesses from risk.

Yet still many businesses erroneously view the escalation of risk & regulatory change as an administrative burden, perpetuating their risk exposure and the threat of non-compliance. Whereas those that see it as an opportunity, not a hurdle, thrive in this new reality. They possess the foresight to seize market and competitive opportunities arising from risk and regulatory change – and they harness the latest GRC software solutions to achieve this.

Businesses that fail to keep up with these rapid advancements in GRC automation remain encumbered by disparate legacy systems that produce siloed data. Worse still, some start-ups in the sector remain reliant on manual processes – such as emails and spreadsheets – making data aggregation processes so convoluted that the information is already stale by the time a report is produced.

In this eBook we explore ten key technology capabilities that every financial services firm – both large and small – should be embracing.

10 GRC Capabilities Financial Firms Can't Do Without!

Here we explore the latest technology capabilities financial services firms are using to automate their GRC processes and improve strategic decision making.

1 Automated Risk Management

Risk management is fundamental in the banking sector and most financial services firms utilise GRC software to digitise & automate their risk management process. GRC software solutions consolidate disparate risk processes, systems, and data sources into a holistic view, providing deep insight into an organisations risk profile, status, and performance.

These intuitive solutions enable organisations to set up a comprehensive on-line risk register, where multiple departments can directly log risks. Teams can utilise online risk assessment templates & questionnaires to calculate the likelihood, severity and impact of risk and generate risk ratings. Transactional & operational data can be pulled into the solution from other systems & data sources via API connections - enabling teams to set Key Risk Indicators (KRI's) and define risk tolerances based on real data. This empowers organisations to define a risk appetite framework & operate within it.

Once the system is established and the risk register is completed, teams can set controls to monitor risk on an ongoing basis and automated notifications & alerts are sent when the degree of risk reaches an intolerable level. Teams can run instant reports and view live dashboards to get a complete overview of their risk profile and drill down into the detail to address problem areas.

Software engages the entire organisation in the risk management process and ensures all stakeholders across the business can log risks and take ownership of risk. This makes risk management more accessible, accountable, trackable, and resolvable - providing visibility to leadership teams - and the automation saves time and valuable resources.

More advanced organisations use risk management platforms to uncover potential opportunities for growth. Instead of simply using the tool to mitigate risk, they use the analytics capabilities to weigh up potential outcomes - enabling them to take a calculated level of risk in pursuit of their strategic objectives.

2 Regulatory Horizon Scanning & Regulatory Change Management

Regulatory compliance is a dynamic process amid ever-changing frameworks, guidelines, and best practices. Mature financial services organisations ease the burden of regulatory change management by using tools that offer automated regulatory horizon scanning and regulatory change management workflows.

These specialist tools link to third-party regulatory content providers and send notifications to stakeholders when an applicable regulation changes. Regulations are linked to any associated internal policies & procedures. Therefore, when a regulatory change occurs, the relevant stakeholder is notified so they can quickly understand which procedures need to be amended to align with the new guidelines.

Some regulatory content providers offer focused information by breaking down regulations and redlining what has been changed and what needs to be done to meet the new requirements. These providers typically work with a team of legal experts to decipher the legislation and make it easier for your business to understand. This cost-saving service removes the need to interpret complex changes in-house and translate them into business process alterations.

Automation also provides a framework for structured change management workflows and a stringent sign-off and approval process - enabling management teams to understand the status of each change. Once the software has scanned the regulatory horizon and notifications have been sent, workflows are automatically triggered to implement the required changes. Having been alerted, stakeholders can document the changes made to meet the requirements, providing a fully time-stamped audit trail of proof of compliance for regulators. This process of proactively anticipating, capturing, and implementing change instils organisational resilience and agility.

Failing to demonstrate compliance with regulations can become an existential threat for small and medium enterprises within the sector. These businesses often lack the resources and brand loyalty required to absorb the financial penalties and reputational damage that ensues. This brings automated regulatory horizon scanning and change management into sharp focus for senior decision-makers in businesses of this size. But with the technology already available within the market, implementing a solution to automate regulatory change management can be fairly quick & simple.

3 Automated Control Monitoring

Most well established GRC teams set up automated control monitoring within their GRC platform to provide immediate visibility into risk exposure. Risk can manifest in so many ways and sifting through reams of transactional & operational data to spot unusual & duplicate transactions, and manual errors would be a laborious and almost impossible task if performed manually - making automated control monitoring a must in the financial services sector.

The banking and financial services sector faces mounting focus on financial and nonfinancial risks – from operational, cyber, and regulatory risks to environmental and social risks. Executives in the sector recognise that the right controls are essential to addressing these risks: in Deloitte's 2021 global risk management survey, 63% of respondents said that controls optimisation, simplification, and coordination will be an extremely high or very high priority for them over the next two years.

Automated control monitoring allows organisations to manage risk proactively using controls based on pre-set rules to detect risk in large data sets and notify the relevant stakeholder. From an irregular transaction to the risk of non-compliance or an audit failure or missed deadline, risks can be detected based on predetermined rules and send alerts to stakeholders.

Controls can be set to flag areas of concern across your entire GRC programme – including missed deadlines, anomalies in data, budget overspend, too many incidents, or when KPIs or key risk indicators (KRIs) reach intolerable levels. This level of automation detects risks that would otherwise have gone un-noticed and provides an extra layer of assurance for risk teams.

In addition, automated control monitoring is a critical component of SOX compliance, as it enables companies to maintain effective internal controls over financial reporting, identify and remediate weaknesses or deficiencies in their control framework, and provides assurance that their financial reporting is accurate and reliable. Internal controls provide real-time monitoring of key financial processes, such as revenue recognition, accounts payable, and payroll, detecting problems early and reducing risk.

4 Strategic Risk Management

Leading businesses in the banking and financial services sector use GRC technology to align their risk management programme with their strategic goals & objectives. This integrated approach allows the organisation to take calculated risks in pursuit of their strategic objectives and detects potential risks that could derail their strategy.

To achieve this alignment, they leverage GRC software that offers risk management and strategic planning capabilities in the same platform. The framework within the tool enables them to map out their strategy by breaking down their goals & objectives into smaller, programmes, projects, tasks, and actions. Each key deliverable is allocated a timeline, budget and KPI's, and any risks are logged and added to the risk register.

As tasks and actions are completed, progress is indicated at each level of the strategic plan. Leaders can easily view the strategy map and its status using simple tree views and dashboards & reports. Automated control monitoring can be set up to flag missed deadlines and budget overspends ensuring problems are addressed quickly. Workflows can be used to add structure to the process, for example when a task or action is completed, the relevant stakeholders are notified enabling them to move on to the next step in the strategic plan.

As part of this setup, organisations can also log any strategic risks which can be monitored as part of their existing risk register within the tool, these can then be linked to tasks, projects, key dependencies, and compliance obligations. Risks can be monitored on an ongoing basis with regular risk assessments, questionnaires, or surveys, and by setting controls based on Key Performance Indicators and Key Risk Indicators.

The execution of any strategy requires some level of risk-taking. By integrating risk management into existing strategic planning processes, organisations can uncover risks to their strategy early and resolve them expeditiously. It also empowers leaders to take calculated risks that help to achieve the strategy. This proactive approach to risk management supports the business in achieving its goals and objectives, rather than just focusing on protecting value – with the risk programme informing the strategy and the strategy informing the risk programme.

5 Policy Management

Regulatory obligations aren't the only thing businesses in the banking and financial services sector must adhere to; there's also a raft of internal policies, procedures, operating guidelines, certifications, and standards that must be adhered to. Maintaining a central repository of live policies & procedures, managing updates & approvals, and understanding who each policy applies to and obtaining attestation can be a cumbersome process for financial services institutions and many organisations choose to implement best-practice policy management tools to simplify the process.

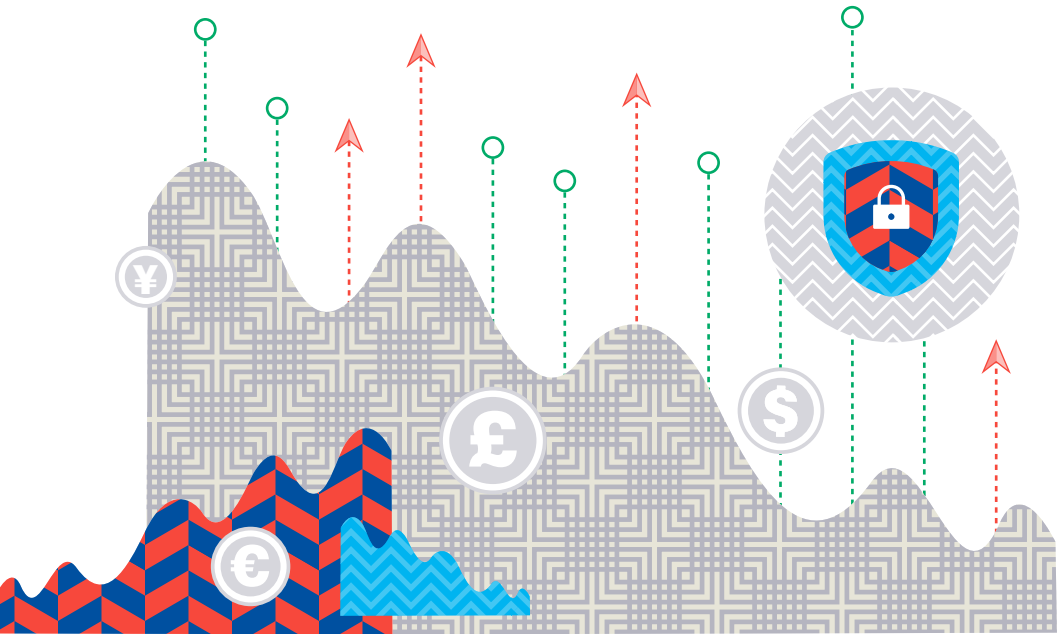
Automated policy management tools usually come as part of a wider GRC platform. The functionality enables organisations to create a centralised policy library. Policies are created consistently using pre-defined templates and essential credentials - like owner, approval date, and expiry date - are captured when policies are uploaded into the solution. Approval workflows can be set up to obtain policy sign off and ensure accountability, and the system provides a time stamped history of all revisions and changes.

Content management functionality ensures policies are current and communicated, and stakeholders can easily access the latest version online. Attestations can be set up to indicate that employees have read and agreed to the policy, this information can be useful for employee tribunals. The solutions also provide access to real time dashboards & reports, together with a robust audit trail, to provide proof of compliance to regulators.

Policy management tools support the entire policy lifecycle across development, maintenance, communication, and attestation. Combined, this functionality enables compliance officers to easily assess the management of ongoing policies, identify areas that require improvement, and action necessary change. Without effective management, policies can soon become outdated, ineffective, or no longer suitable for dynamic business needs – leaving the organisation vulnerable to liability.

6 Cyber & IT Risk Management Tools

With many processes relying unreservedly on data & IT systems, cyber risk is high on the agenda for most financial services organisations as they grapple with the exponential growth of new and emerging threats. In its 11th Risk Barometer, Allianz ranked cyber incidents (44% of responses) as the most important business risk globally for 2022 – pushing it up from third in 2021. This return to the top spot was attributed to a series of high-profile ransomware attacks, combined with problems caused by accelerating digitalisation and remote working. According to research by Sophos, in 2021 over half (55%) of financial services businesses were victims of at least one ransomware attack, up from 34% the previous year, representing a 62% rise in these threats in just one year.



Due to the vast amounts of sensitive information these financial services organisations hold and the escalating risk of cyber-attacks, organisations in the sector have blazed a trail by reinforcing cybersecurity with technology.

Cyber & IT risk management solutions offer a framework to build an online cyber risk register and KRI's can be set against IT data held in other systems by pulling it into the solution via API's - enabling organisations to set up automated controls to flag problems. Cyber risk tools enable teams to roll out online risk assessments, surveys and questionnaires with all data feeding directly into the tool - facilitating ongoing risk monitoring.

In addition, cyber risk tools offer a best-practice online cyber incident reporting process. Automation allows teams to manage incidents through to resolution efficaciously by implementing mitigating actions and setting robust controls to eliminate further occurrences. Reports can easily be viewed to determine the source of recurring incidents to prevent future instances.

GRC solutions that offer cyber risk & compliance capabilities also offer best-practice frameworks to manage complex cyber-related compliance requirements like ISO 27001, NIST, HIPAA, PCI DSS, SOC 2 and GDPR, simplifying compliance with these requirements.

Traditionally, boards have associated cybersecurity solely with IT – a rigid approach that fails to recognise that it is a business risk, not just a technology issue. GRC software has shifted this antiquated mindset by allowing organisations to integrate cybersecurity into an enterprise risk framework, providing visibility of cyber risk across the organisation.

7 ESG

Demonstrating ESG credentials is becoming a key concern for financial services institutions. Although businesses in the banking & finance sector don't have the same impact on the environment as more invasive industries like manufacturing & energy, the social and governance side is of huge relevance for organisations in this sector. With the pressure to satisfy ESG (Environmental, Social, and Governance) issues greater than ever, they can't afford to overlook them – a potentially costly oversight that might result in financial penalties and reputational damage.

In Deloitte's 2021 global risk management survey of financial institutions, 47% of respondents said it will be an extremely or very high priority for their business to improve their management of ESG risk over the next two years.

As the importance of environmental and social responsibility gains momentum, organisations are under mounting pressure from all stakeholders – governments, regulators, consumers, staff, third parties, and investors – to be more transparent about their ESG impacts and many organisations are utilising GRC software solutions with ESG capabilities to monitor ESG requirements and provide data to back up their bold claims.

To successfully demonstrate commitment to ESG initiatives, organisations use an ESG software solution to set goals and define what success looks like. They use the risk management functionality to manage any associated risks and use the compliance capabilities within the tool to ensure compliance with anti-bribery & corruption laws, environmental obligations, regulations, and standards.

A GRC solution that's augmented with ESG capabilities provides a best-practice framework to collect and aggregate relevant data in the required format by integrating data from other systems via APIs and rolling out online forms & questionnaires to collect new data. Once this collection process is completed, the software ensures the resulting information is consistent, consolidated, analysed, and communicated using comprehensive functionality including regulatory horizon scanning, compliance monitoring, risk management, policy management, automated workflows & alerts, and automated control monitoring.

This single source of truth underpins a holistic ESG programme that can grow and evolve with your business, engage stakeholders, and demonstrate that your business considers people and the planet as part of its operating model.

8 Online Incident and Near-Miss Reporting

To understand and mitigate what might happen in the future from a risk perspective, you must look to the past - and analysing historic incident & near-miss data is a great way to do this. Your incident log provides the insight, foresight, and oversight needed to understand what events are resulting in risk. From major incidents such as cyber-attacks & outages to minor incidents such as slips & trips, by analysing the data, organisations can delve into what risks caused the incident and what steps they can take to prevent future occurrences.

To effectively link your incident log to your risk management programme it is best if both programmes are managed in the same GRC platform. Online forms & templates within the tool enable staff at every level of the organisation to report risks from anywhere using the internet or mobile apps. These consistent reporting processes ensure even the smallest incidents and near misses are captured and used to understand trigger events before they escalate.

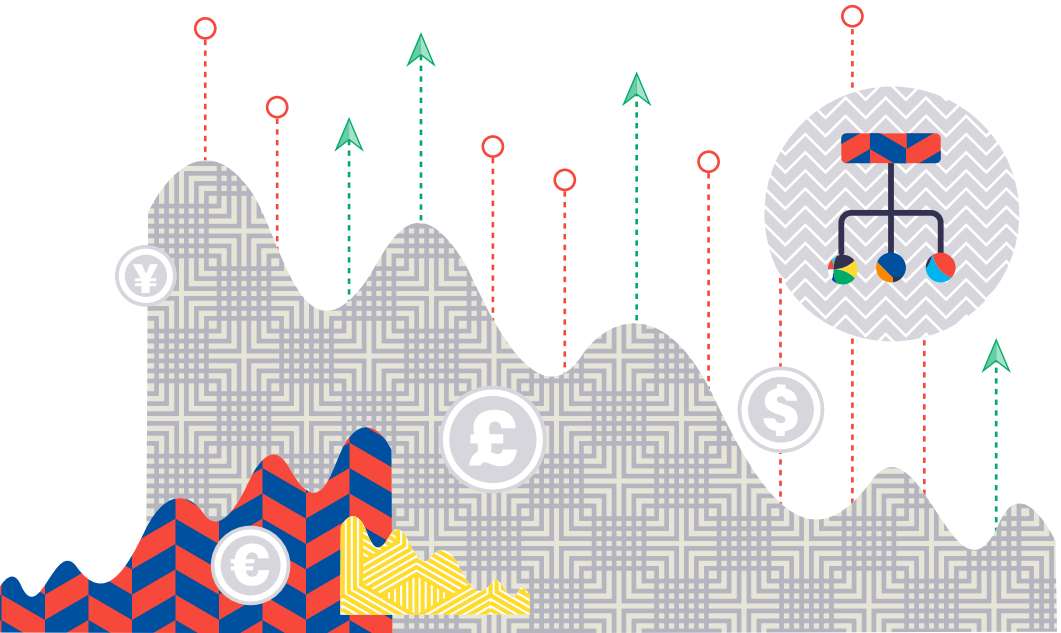
When users log an incident they can upload photographs, screenshots, and URLs directly into the system and by linking incidents to business units, systems, controls, and risks, they can build a clear picture of where risks are originating. Incidents can also be linked to relevant policies & regulations to identify compliance risks, with everything date and time-stamped for a comprehensive audit trail. Business data can be integrated via APIs, allowing departments and staff members to be linked to incidents for improved planning, administration, recording, triaging, routing, investigating, tracking, and closure.

When using GRC software for incident management, transparent protocols and automated workflows & alerts allow compliance officers to establish a consistent process for staff. This provides the structure to conduct thorough investigations, root cause analysis, and manage incidents through to resolution via a central point of oversight. This single pane of glass view supports the holistic management of incidents by engaging all stakeholders. A collective understanding of the value of risk management ensues, together with a determination to address it proactively, helping to foster a risk culture that's embraced by all.

9 Third-party Risk Management

Every organisation relies on a network of third parties to keep their operations running smoothly. Even smaller organisations can have dozens of relationships that they depend on for goods, services, and technology - and larger financial services firms can expand into the hundreds or even thousands. Without a central point of oversight, and a consistent way of rating and monitoring vendors, many organisations leave themselves vulnerable to unforeseen risk.

That's why many organisations in the financial services sector utilise specialist third party or vendor risk management tools to monitor supplier performance, compare vendors, and understand the associated risks.



These solutions enable staff from across the organisation to log any existing or potential vendors or third parties within the solution using online forms, capturing key details regarding contract length, cost, relationship owner and any SLA's or KPI's. This makes it easy for decision makers to compare vendors and allows them to set controls with automatic notifications to monitor performance against KPI's and SLA's.

Third-party risk management solutions offer online forms to perform key tasks including supplier onboarding, vendor risk assessments, questionnaires, and surveys - with all results logged in the system against the relevant vendor. Any potential risks can also be logged against each vendor and monitored on an on-going basis. Some solutions allow you to pull in live transactional & operational data relating to supplier performance from other systems & data sources - allowing risk teams to automatically monitor supplier performance against KPI's and SLA's and receive notifications of poor performance so it can be addressed.

Around 70% of respondents in Deloitte's Global Third-Party Risk Management Survey 2022 indicated that they want to exploit synergies across third-party management processes to drive efficiency - implementing a best-practice third party risk management programme is the best way to achieve this.

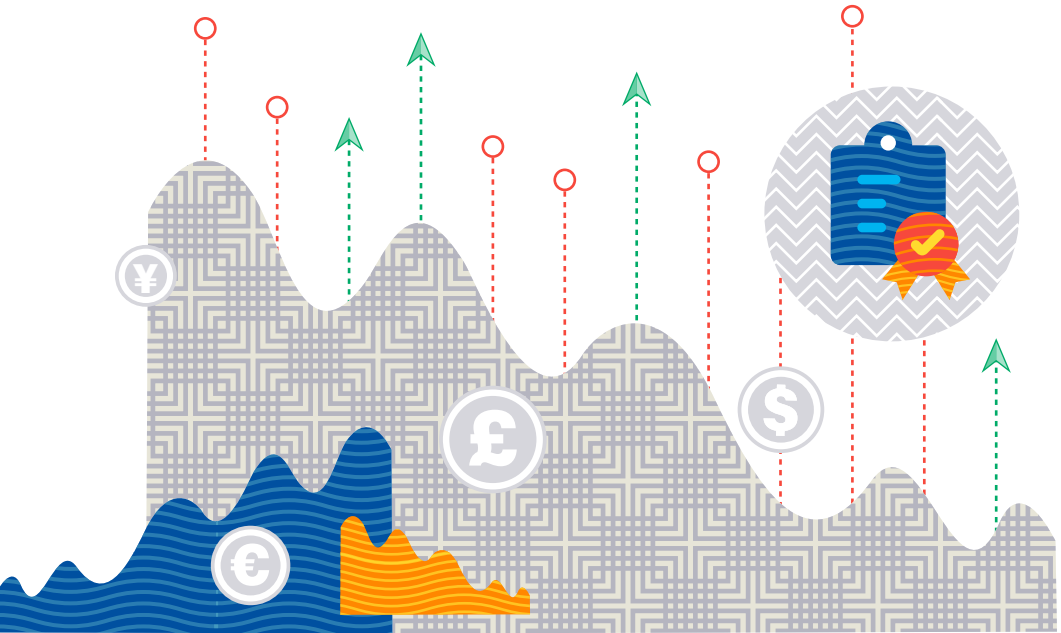
The dashboards & reports available within the solutions give risk teams complete oversight of each vendors performance and any potential problems. With all this information stored centrally and easily accessible, the software automatically creates an auditable vendor selection process.

10 Audit Management

Financial services organisations are privy to a whole host of regulations, standards, and policies and as a result are subject to regular audits to ensure they are operating in line with guidelines. Keeping track of upcoming audits and tracking the outcomes of previous audits can become a challenge for organisations and many businesses in the financial services sector use GRC software platforms that offer audit functionality to ease the burden and automate the process.

The tools let you build a centralised register of all your audits online and schedule them upfront. The system automatically sends reminders to the relevant stakeholders when audits are due so the necessary steps can be taken - driving accountability. Findings of all audits are captured in the tool and automated workflows are used to implement recommendations and log actions to complete the audit cycle.

Audit management software helps organizations to identify and mitigate risks more effectively by providing real-time monitoring of key processes and controls. This enables auditors to identify potential issues before they become significant problems. Audit software can also support compliance activities by helping organisations to comply with regulatory requirements and industry standards by providing a framework for documenting and reporting on audit activities.



This comprehensive process provides a complete history of all your audits and their findings and any outstanding actions. Real time dashboards and reports make it easy to spot trends, identify problems, and conduct investigations. Many tools enable organisations to link audit to compliance obligations and risk management - adding another layer of depth to the process. This comprehensive mapping enables businesses to understand the risks relating to a failed audit or the impact of non-compliance.

Small to mid-sized organisations who adopt these structured audit processes early will be well placed to expand and mature their practices in line with business growth.

GRC Technology: Create an Agile Business Model Based on Risk Intelligence

GRC solutions that automatically manage emerging and established risks using comprehensive functionality are not the preserve of multinationals. Their vast resources and complex requirements have simply allowed them to provide the blueprint for successful adoption by small to mid-sized firms. The right technology implemented correctly can help businesses of all sizes to operate efficaciously in what is a complex, highly regulated, and risky environment.

Risk management is not a linear process, you will require different capabilities at different stages of the risk management lifecycle. As your business grows and your risk programme matures, you will need a GRC solution with the agility and functionality to evolve with it. To achieve this, you must integrate software that offers multiple capabilities across risk, compliance, audit, incident, strategy planning and ESG in one platform. This will ensure organisations can align these processes in the future and prevents a siloed approach that does not offer the complex mapping needed to visualise how these processes impact each other.

Smaller organisations should learn from the robust best-practice processes that have been developed to meet the requirements of larger businesses. Implementing these comprehensive frameworks enables firms to link their GRC processes to their strategic plans in one platform providing critical insights into how these processes affect each other. This allows businesses to take risks in pursuit of their objectives and better understand the risk of non-compliance.

If you are still using spreadsheets and manual processes, it might be time to investigate a GRC platform that can drive risk-informed decision-making using data that's aligned with your business objectives and KPIs.

About Camms.

Camms offers a cloud-based SaaS GRC solution that aligns with organisational strategy, enabling organisations to manage their GRC programme in line with their strategic goals & objectives. The solution uses a modular approach, allowing financial services institutions to scale and mature their GRC programmes at their own pace. Some of the core capabilities include:

Risk management:

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

Compliance management:

House a comprehensive obligations library of relevant regulations, legislation, policies, and internal procedures. Set a structured process for version control, approval, ownership, 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.

Strategy management:

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

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:

Schedules and manages internal and external audits and formalises the results and required actions. Provides a complete history of all your audits and their findings and any outstanding actions.

Cyber and IT risk:

Manage the complex framework of compliance requirements and risks related to ISO standards and data privacy laws like GDPR. Monitor IT risk and track cyber related incidents.

API integrations:

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

Stakeholder dashboarding:

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

Analytics & reporting:

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

Managing these different functions in a centralised platform fosters collaborative working and the sharing of data across teams. It enables communication from the top-down and bottom-up and ensures operations follow best practice processes to keep leaders, auditors, and regulators satisfied.

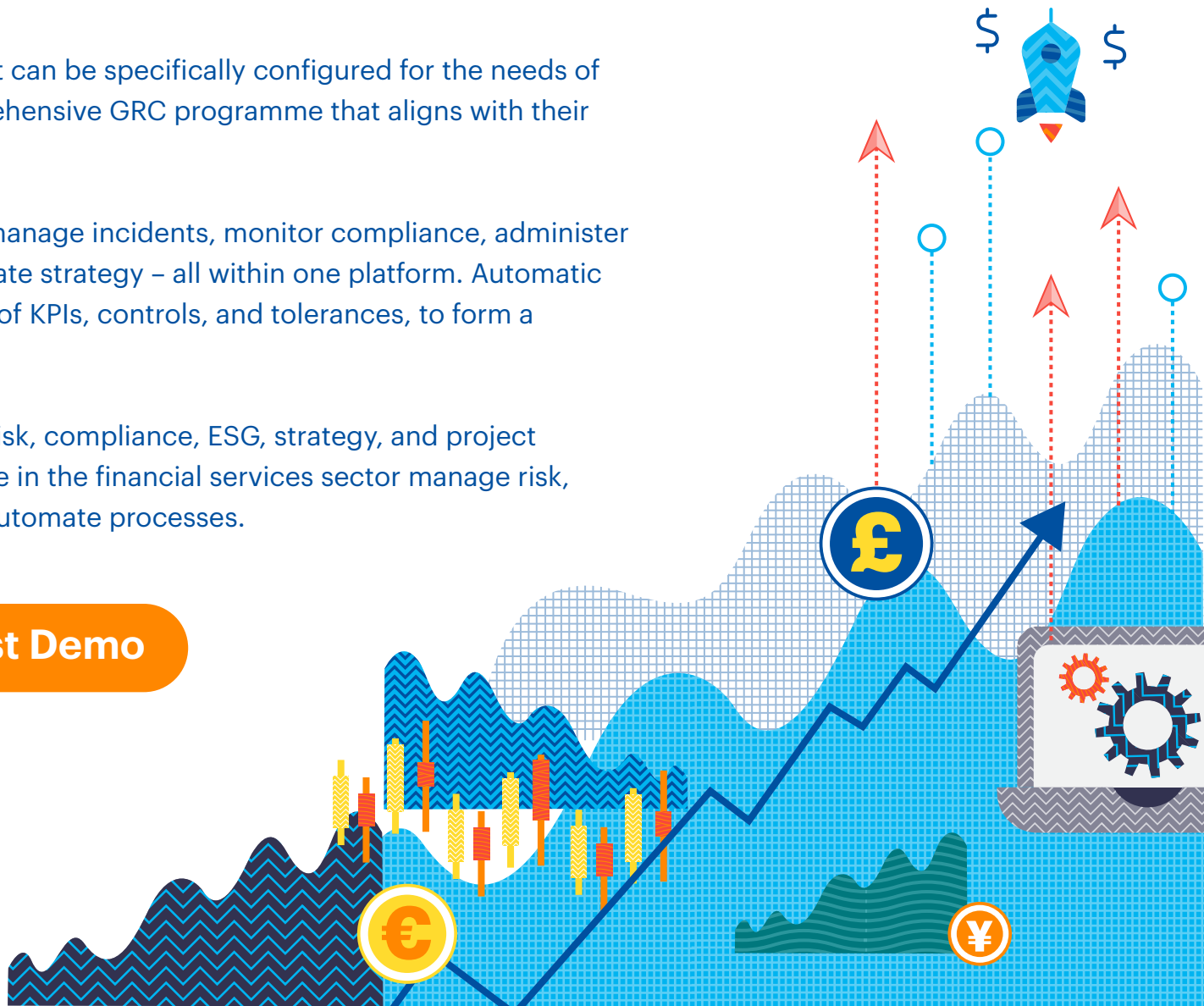
Discover How Camms Is Helping the Financial Services Sector to Automate Their GRC Processes

Camms offers a cloud-based SaaS solution that can be specifically configured for the needs of the financial services sector to set up a comprehensive GRC programme that aligns with their strategic goals & objectives.

Set up obligations libraries and risk registers, manage incidents, monitor compliance, administer policies & regulations, and roll out your corporate strategy – all within one platform. Automatic workflows & alerts link to a defined framework of KPIs, controls, and tolerances, to form a complete end-to-end solution.

With integrated solutions across governance, risk, compliance, ESG, strategy, and project management, Camms software is helping those in the financial services sector manage risk, make the right decisions, and streamline and automate processes.

Visit Website **Request Demo**



Camms.

Software to Change Tomorrow.