From isolated processes to integrated alignment: **Automating risk management and incident reporting**

Camms.

A Riskonnect company

INTRO

When it comes to risk management and incident reporting, many 'incidents' are actually 'risks' that have materialised into full blown incidents - so it's no surprise that integrating these areas can bring a wealth of benefits to an organisation. But why can't we always identify risks first so they can be managed before they become full-blown incidents? The answer to this valid question is simple: we can't always tell what came first, the risk or the incident – a common chicken or egg scenario that arises due to the subtle or hidden indicators of risk, making them difficult to identify early. This often means that an unexpected incident that has a sudden and significant impact on a business will prompt an organisation to add it to the risk register.

Amid these blurred lines, we can clearly see that incidents are a rich source of information about risks and vice versa. To harness risk & incident data to provide strategic insights that guide the business, you must look beyond proactively identifying risks in isolation by aligning risk management with incident reporting.

This joined-up approach ensures information about incidents, hazards, or near misses is captured and documented. The resulting data can then be leveraged to create risk indicators that shine a light on things like process gaps and system failures. By mapping these functions, firms can also easily identify risks that turn into incidents - enabling them to implement controls and measures to prevent recurrences and reduce risk.

To effectively integrate risk management and incident reporting, businesses should amalgamate their processes using GRC software to automate and align both functions. In this eBook we explore all the features of best-practice risk management & incident reporting processes and explain how these areas can be integrated to provide data driven outputs to guide decision-making.

What does best-practice risk management look like?

Best practice risk management involves a systematic approach to identifying, assessing, monitoring, and mitigating risks that could impact a business. The goal is to minimise the impact of risks and maximise opportunities by managing them proactively.

Let's take a tour through the key aspects of a risk management programme

Risk Register

Most risk management programmes start out with a risk register. A risk register is a central repository of organisational risks that allows stakeholders to monitor each identified risk and track relevant information linked to it, so it can be monitored, analysed, and controlled or mitigated. Most risk registers share common elements that allow risks to be rated and compared, including description, categories, analysis, probability, priority, response, and ownership.

By building and maintaining a comprehensive risk register, firms can elevate the risk management process by providing stakeholders with access to key information on risk exposure – allowing firms to decide where they will allocate funds and resources to reduce risk.

Here are some of the advantages of maintaining an active risk register:

- **Risk visibility:** A risk register acts as an accessible list of risks allowing stakeholders to view all potential threats and opportunities - improving organisation-wide awareness and understanding.
- **Risk assessment and prioritisation:** A risk register typically enables employees to evaluate risks based on their likelihood and impact. This helps to prioritise risks, ensuring the highest-graded ones receive appropriate attention and resources and understanding.
- **Risk response planning:** A risk register typically outlines mitigation strategies, controls or response plans for each risk - providing pre-defined actions to address each risk, minimising the impact.
- **Informed decision-making:** With all risks clearly documented and assessed, decision-makers can make more informed choices, balancing potential risks against expected benefits or costs.
- **Accountability:** A risk register often assigns ownership of each risk to a specific individual or team - enhancing accountability. This clarity helps ensure that risks are actively managed rather than overlooked.
- **Continuous improvement:** A risk register allows for the tracking of risks over time, documenting how they evolve and how they are managed. This historical data can be harnessed to improve future risk management efforts.
- **Compliance and reporting:** A risk register facilitates regulatory compliance by providing documented evidence of risk management activities.

Risk Framework

To gain clarity amid the avalanche of internal and external risks your business is exposed to daily, you must build a robust risk management framework. This provides a structured, systematic approach to categorising, assessing and prioritising risks based on their likelihood & impact – the benefits include: more informed decision-making, better resource allocation, and optimised risk management oversight. A good risk framework includes methods for:

Categorising risk:

Businesses face a wide variety of risk types including strategic, compliance, operational, financial, Cyber & IT, third-party, and reputational. This classification helps your business avoid any unexpected incidents by establishing a structured and consistent approach to identifying and documenting each risk type, these can even be housed in separate interconnected risk registers in larger organisations.

Assessing risk:

A comprehensive risk framework includes criteria for assessing the likelihood of a risk occurring and the potential impact if it does - through regular risk assessments and business impact assessments. This helps to quantify risks with precision, which drives effective prioritisation. Frameworks typically leverage qualitative and quantitative methods to achieve this, providing a balanced view of the potential threats.

Prioritising risk:

Each risk is assigned a score based on its likelihood and impact, which helps in rating the risk – such as high, medium, or low – and determining its priority. To ensure the ratings align with the business's overall strategy and objectives, the framework should consider your risk appetite (the amount of risk you're willing to accept) and risk tolerance (the acceptable variation in outcomes) as well as any long-term strategic goals & objectives which may require you to take a certain degree of risk.

Key Risk Indicators

Each risk should have clearly defined Key Risk Indicators (KRI's). KRI's are essential data that indicates the current level of each risk, and they provide early warning signs of increasing risk exposure. KRI's can be based on the results of risk assessments or based on transactional or operational data from other systems & departments. Incident reporting data can also be used as a key risk indicator.

By constantly monitoring risk levels using KRI's, firms can easily monitor fluctuating levels of risk and take action to reduce risk in areas that are deemed too high and exceed their risk appetite. This risk management 'alarm system' underpins the process of monitoring and predicting potential high-risk areas and taking prompt action to prevent or mitigate their impact before they materialise into unwanted incidents – empowering you to:

- Identify current risk exposure and emerging risk trends.
- Operate within your risk appetite and desired tolerance levels.
- Highlight control weaknesses and allow for the strengthening of poor controls.
- Implement operational risk management that adds strategic value.

Monitoring Risk

Risk monitoring is the ongoing process of tracking risk levels against KRIs to ensure they remain at a tolerable level and don't impact the business's ability to achieve its objectives. By ensuring that risk levels are continuously monitored and ensuring that any changes in the risk environment are promptly identified and addressed - you can maintain control over your risk exposure. Risk monitoring is a continuous process, it must happen at regular intervals so businesses can understand what is causing risk levels to rise or fluctuate.

A fundamental element of impactful risk monitoring is regular risk assessments that proactively identify, evaluate, and prioritise risks that could impact your business's operations and objectives. By continuously analysing potential risks to determine their current level and their likelihood and potential impact, you can implement appropriate measures to manage or mitigate them.

Control Library

A control library is a comprehensive list of controls that a business has developed and implemented, to neutralise or reduce risks. These controls are usually measures, policies, procedures, step-by-step processes, safety & security equipment, or regular checks - designed to prevent, detect, or correct risks that could negatively impact the organisation.

With the library in place, and robust controls set to keep risks within tolerance levels - the business should carry out regular control checks and control testing to ensure the controls are effective in preventing the risk they were designed to mitigate.

Risk Escalation & Treatment

Even with the best risk mitigation efforts and effective controls there will likely be occasions where risk levels rise, and 'risk' needs to be escalated and treated. Firms need to clearly define an escalation route, and the actions and steps taken to reduce the risk need to be fully documented.

Businesses should adopt a fluid approach that allows them to escalate risk, instigate treatment actions without delay, and manage cases through to completion.

Risk Reporting

An efficient risk management process requires access to information that guides business decision-making. This should be facilitated by detailed risk reporting - alerting stakeholders of high-risk areas and failed controls so they can decide where to allocated budget and resources to reduce risk. The aim of creating clear and accurate risk reports is to provide the right information to the right people at the right time so that they can manage risk effectively and without delay.

Robust risk reporting processes provide visibility of your risk exposure, risk mitigation efforts, and control effectiveness. Accurate and timely information allows stakeholders to spot trends and make informed decisions that drive improvement and lower risk levels.

Automating Risk Management with GRC Software

Risk management that relies on outdated manual processes like emails, spreadsheets and physical meetings results in sluggish processes and siloed data - depriving businesses of quality risk-related information. Manual processes are too rigid and lack automation and integration - perpetuating a reactive response. These clunky, time-consuming, and error-strewn processes lack the efficiency and connectivity needed to establish a proactive and integrated approach to risk management that considers the entire organisation and its strategy.

GRC software overcomes these constraints by bridging the gap between the business and its risk management responsibilities and automating processes. The enriching result is a single source of truth that provides a comprehensive and accessible view of risk management performance and instils the agility to manage risk proactively. It also offers a transparent view of your risk programme across all areas of risk including operational, cyber, compliance, and third-party risks.

Automated functionality facilitates joined-up, continuous risk identification, analysis, monitoring and reporting that engages employees and provides a holistic view of risk.

Let's explore how GRC software can automate the key aspects of a risk management programme

Automated Risk Register

GRC software powers the creation of a digital, searchable 'risk register' with multiple risk types that can be easily filtered and accessed online by multiple employees concurrently. This allows firms to capture different risk categories separately and run combined reports to view risk holistically. Predetermined templates can be customised to include additional information that needs to be captured when logging different risk types. Standardised fields, menus and drop-downs ensure risks are logged accurately and consistently.

An impact and probability score is calculated for each risk, before being mapped to the related mitigating controls and business units that will likely be impacted if the risk materialises. This allows stakeholders to analyse risk granularly and escalate it according to the wider business impact.

Standardised Risk Frameworks

GRC software provides predefined frameworks and templates that allow you to categorise and rate risks according to common risk management frameworks and rating standards. The ability to standardise risk categorisation and prioritisation allows management to make risk-informed decisions, allocate resources more effectively, and work within a predefined risk appetite.

Automated Risk Monitoring

As well as monitoring risk through regular risk assessments, GRC software can also detect risk in large operational and transactional data sets. Data from other systems and data sources can be pulled into the GRC tool via API integrations and firms can use predetermined rules to indicate when KRIs are high, before sending automatic alerts to stakeholders to address the problem.

Control Automation

GRC software enables organisations to maintain a control library of the controls and measures they currently have in place to reduce each risk. Whether the control is a policy, procedure, a regular check or a piece of safety or security equipment, it should be logged in the library and linked to the corresponding risks.

The software also facilitates firms to carry out regular control checks and testing in the platform. Automated workflows send out online control check forms for operational staff to complete. All data entered feeds into the GRC platform, and any control failures, gaps or inefficiencies can be easily identified and addressed.

GRC software provides risk teams with the agility to achieve robust internal monitoring and testing of the controls that oversee high-risk operational processes, with each risk easily mapped to the corresponding controls.

Automated Risk Assessments

GRC software completely automates the risk assessment process. Firms can use the platform to establish a variety of online risk assessment forms for each risk type. Automated workflows can be used to send out the forms via email on a regular basis to the relevant employees. Chaser emails are automatically sent when forms are not completed by the deadline.

Employees of all levels can use the GRC tool to enter risk assessment data with all data feeding directly into the GRC tool to effectively monitor risk levels and current risk exposure across the entire enterprise.

Integrated KRIs

GRC software supercharges KRIs. KRI data can be intuitively fed into the software via API integrations with other data sources and systems – cutting back on admin and providing a single source of truth. For firms that combine risk management and incident reporting in the same platform, they can use incident data as a 'Key Risk Indicator' to alert the business when risk levels are high - based on an increase in incidents in a particular area.

Automated Escalation & Remediation Workflows

When risk- data is stored centrally using GRC software, workflows can be automatically defined for approvals, escalations, and remediating actions. When a risk level goes 'into the red', automatic workflows escalate the risk to the relevant stakeholder and a step-by-step 'process workflow' kicks into action to ensure the risk is resolved promptly and all remediation steps are fully documented.

Permissions Hierarchy

GRC software enables the entire organisation to feed into the risk management programme whilst adhering to a strict user permissions hierarchy. This broadens the scope of risk by enabling staff of all levels to complete simple tasks like risk assessments and control checks via online forms – with all data feeding into the platform. A record is maintained of who entered what and when to ensure accountability. Staff only see the data and tasks relevant to their role, preventing them from getting overwhelmed by large amounts of data and protecting sensitive information.

Personalised Dashboards

Each user will have their own dashboard showing their outstanding actions and tasks and key metrics relating to their area. More senior employees will be notified of risk escalations and will have access to dashboards & reports relating to risk exposure and control status in their teams. Senior leaders and risk professionals can get a complete view of risk exposure across the entire enterprise. Dashboards can be tailored to each user profile - ensuring they can get an instant view of key metrics and outstanding actions and a personalised 'to do' list ensures all actions and tasks are completed on time.

Automated Risk Reporting

The live dashboarding and automated reporting available in GRC software provides clear visibility of your risk profile and highlights high-risk areas and control gaps. Access to this accurate information allows stakeholders to identify trends, spot anomalies, and make informed decisions that drive improvement. By streamlining the risk data aggregation & reporting process, time-critical information is reported centrally when needed, with dashboards designed to highlight priority areas. This automation eliminates data manipulation and manual reporting efforts, leaving risk teams with more time to analyse the data and drive meaningful change. Teams can run reports on risk levels, control effectiveness, and resolution status, and they can easily view the data via interactive visualisation outputs like dashboards, heat maps and bowtie analysis.

What does best practice incident reporting look like?

Best practice incident reporting provides the structure to document events accurately, investigate them thoroughly, manage them to a full resolution, and use them to prevent future occurrences. To achieve this, you must recognise that there's no one-size-fits-all approach to impactful incident reporting. Amid the diverse business landscape, organisations are exposed to different incident types – such as cyber incidents, operational incidents, system downtime, health & safety related accidents, and confidential incidents like whistleblowing & disclosures. Each incident type will likely require its own form, escalation routes, priority ratings, and resolution process.

Let's delve into the key aspects of a best-practice incident reporting process

Logging Incidents

Making it easy for staff to log incidents is crucial for your business to track, respond to, and analyse events that may undermine & disrupt operations, security, or compliance. Each incident type should have a specific logging process to capture the necessary details based on organisational policies or regulatory standards for the incident type. For instance, when logging a cyber incident involving compromised data, you must adopt a process that complies with appropriate laws and regulations, such as the General Data Protection Regulation (GDPR) in the EU and UK. As well as capturing critical detail about the incident and who was involved and when it happened, staff should also be able to include photos or documents to ensure all evidence is documented. Firms must endeavour to capture all relevant details systematically and consistently to ensure incident data can be easily reported on and compared across different departments and sites. Proactive organisations also choose to capture hazards and near misses. This helps them to implement measures to prevent incidents before they occur.

Categorising & Prioritising Incidents

Incident classification and prioritisation are interrelated processes that help you assign the appropriate resources, actions, and timelines to resolve incidents quickly.

Categorisation

Incidents should be categorised into categories and subcategories that reflect your business's services, processes and priorities. Many businesses choose to categorise by type for example, health & safety incidents, cyber & IT incidents, supply chain incidents, system downtime, or discreet HR related incidents like whistleblowing & disclosures. Having categorised an incident using the relevant criteria, you can allocate the right resources to respond effectively using standardised procedures tailored to each incident type.

Prioritisation

The process of accurately ranking incidents requires the creation of predefined criteria and metrics linked to their severity and business impact. This provides the structure to prioritise critical incidents, which if not addressed promptly can cause significant disruptions, such as downtime, data loss, or reputational damage. Clear escalation routes should be defined for each incident type so it can be prioritised - ensuring faster resolution times for incidents that require immediate attention.

When incident categorisation and prioritisation dovetail seamlessly, incidents are escalated to the right individuals so they can be resolved quickly. Capturing and ranking incidents consistently generates valuable data that can be analysed to identify trends and areas for improvement. This data can also be leveraged to elevate forecasting and planning to reduce future incidents, improving overall operational resilience.

Escalating incidents

Escalating incidents to the right teams and individuals within an appropriate timeframe is key to resolving them quickly. Sometimes incident resolution demands a larger team, specialised knowledge, or more senior skills. Therefore, as part of your incident process it is important to establish the escalation routes for different incident types upfront to ensure new incidents are escalated promptly without delay. By escalating an incident to continue the investigation and diagnosis using a more experienced or skilled resource it can be quickly brought to the attention of the appropriate personnel, minimising downtime, reducing operational impact and ensuring regulatory compliance.

Escalation routes are not linear. Each incident type requires the creation of a defined pathway that aligns with its unique characteristics. By assigning clear responsibilities to specific roles or teams, these transparent processes provide accountability and prevent incidents from falling through the cracks. For instance, confidential incidents like whistleblowing and disclosures require discreet escalation routes that facilitate anonymous reporting, with the right people gaining access to the right data. Without this, the integrity of the case will be compromised, potentially leading to reputational damage.

Case Management

Incident case management is a structured process comprised of a sequence of connected, repeatable phases in the life cycle of an incident. These step-by-step processes ensure incidents are escalated to the right people, managed efficiently, resolved quickly, and documented properly.

A typical incident case management process might involve the following phases:

- **Identification:** An incident, hazard or near miss is identified by a staff member.
- **Logging:** Details of the incident are logged using the incident reporting process, including description, time, affected systems, and any photos, videos, documental evidence and voice recordings are captured.
- **Categorisation & Prioritisation:** The incident is then categorised based on its type and assessed for its impact and urgency, which determines its priority rating.
- **Escalation:** The incident is then assigned to the appropriate team or individual based on the category, type and severity of the incident. The incident is then analysed to determine its severity, scope, and potential impact on operations, and it can be scalated further or sent to specialist teams if required.
- **Investigation:** The assigned team or individual investigates the incident to identify the root cause – all investigations and findings should be fully documented.
- **Resolution:** A detailed plan is formulated using the data available and executed by the relevant stakeholders to resolve the incident.
- **Closure:** The resolution processes and lessons learned are documented for future reference. The incident is reviewed, and if everything is satisfactory, it's officially closed.
- **Review:** A post-incident review is conducted to assess the incident, the response, and the outcome. The team identifies what went well, what didn't, and how future incidents can be handled better.

Incident Rate Reporting

Reporting on incident rates, hazards and near misses to understand their frequency and root causes is essential to prevent future occurrences. Therefore, being able to run reports on incidents and visualise the results is essential to support the organisation to lower incident rates.

It is important to understand who is involved in incidents and where they occurring and what is causing them to prevent future incidents.

Automating Incident Reporting with GRC Software

GRC software provides a best practice system for incident reporting by ensuring data is captured consistently for complete alignment, and all associated events are managed to a full resolution via flexible case management workflows. This innovative approach streamlines the incident management process, reduces human error, improves response times, and provides real-time data to all stakeholders.

The process is fully automated – from identification and logging to closure and review, and a fully time-stamped audit trail of the incident lifecycle is provided. This fosters a collaborative, structured approach that ensures incidents are escalated and resolved without delay. The software offers personalised dashboards enabling staff to view their outstanding actions and tasks relating to incidents – ensuring nothing slips through the cracks. A wealth of reporting outputs enables teams to uncover the root causes of incidents – enabling firms to implement measures to reduce future occurrences – this proactive approach reinforces the business in the long term, rather than treating incidents as a moment-in-time-event.

Here are some of the ways GRC software can streamline and automate the incident reporting process

Online Incident Logging

GRC software provides a centralised platform where staff can log incidents, hazards or near misses via online forms that are tailored to different incident types using predefined fields and templates. Vital data is captured regarding date and time, employees involved, and processes affected - along with evidence, such as images, URLs, and files. All the data from the digital forms feeds directly into the platform – building a searchable database of real-time incident data.

Data governance can be used to enforce validation rules that determine whether logged data meets specific criteria, elevating the quality & format of the information recorded by staff. By capturing incident data consistently and accurately in a centralised platform - rather than storing it disparately across different systems or departments - it becomes easier to track and analyse.

Automated Incident Categorisation & Prioritisation

GRC software enables firms to set predefined rules and frameworks for consistent incident categorisation based on the data entered when the incident is logged. These categories can be customised to align with your business's specific risk landscape, allowing for all relevant incident types to be accounted for. Having contextualised incidents – such as the business unit affected, regulatory requirements, or existing controls – the software can automatically prioritise them according to their severity and business impact.

Automated Incident Escalation Workflows

With information related to the source and cause of incidents stored centrally, GRC software escalates each incident to the appropriate individuals or teams using predefined workflows and notification emails, so they can take timely action. Incidents will take a different escalation route based on their type, category, and priority ensuring the right stakeholders are notified or informed. Incident data is enriched with context from risk registers and compliance obligations, facilitating informed decision-making during the escalation.

Empowered by real-time dashboards and reports that offer a centralised view of the escalation status, stakeholders can view the escalation route and current action owners, ensuring clear accountability and responsibility throughout.

Automated Case Management Workflows

GRC software allows stakeholders to log all remediating actions for an incident centrally, and fully document the resolution process. This enriching data is collected through tailored case management workflows that align with specific incident types. From conducting route cause analysis to implementing remediating actions & tasks, these systematic, technology-driven processes streamline incident response and resolution, allowing for a faster, more efficient, and consistent approach.

Dashboards & Reporting

When using GRC software to facilitate your incident reporting process you can run a wide variety of incident reports at the touch of a button. Report on incident rates across different business sites and teams, investigate common causes, and view stats on resolution status and timelines. Personalised dashboards are available for each user profile - enabling them to view incident stats and outstanding actions relating to incident escalations and remediating actions & tasks.

10 Benefits of Integrating Risk Management & Incident Reporting in a GRC Solution

Proactive businesses anchor incident reporting in the risk management process by managing these two vital disciplines in the same fully integrated GRC platform - and the benefits are compelling. This joined-up approach will empower your business to build an incident-informed risk management programme that links risks to related events by consolidating disparate processes, systems, and data sources into a single point of oversight.

Here are 10 advantages of integrating risk management & incident reporting in a GRC platform

1 Identify Gaps in your Risk Register

Having wedded risk and incident data in a unified platform, your risk teams can identify gaps in the risk register. Teams can use incident data to uncover the typical source and root cause of logged incidents, hazards, and near misses. The causes of these underlying incidents can be added to the risk register and controls can be implemented to prevent similar incidents reoccurring.

2 Enhanced Risk Oversight

Mapping incident reporting and risk management will allow the organisation to construct a panoramic view of the risk landscape by understanding - what risks have turned into full-blown incidents, how they've impacted the organisation, and how long they took to resolve. This will help firms to anticipate the likelihood and potential impact of risks in the risk register by examining historical incident data.

3 Enhanced Key Risk Indicators

Incident data is often a vital source of information for Key Risk Indicators (KRI's) which is why it is vital that these functions are integrated. For example, if you are managing the risk of theft and you have lots of incidents of theft, this incident data will signify that the risk level is high, and the controls are ineffective – triggering control checks & risk remediation workflows.

4 Single Source of Truth

Managing risk and incidents in the same platform will ensure you have a single source of truth. If the processes are managed separately, risk levels may look low and controls may be showing as effective, but incidents might be sky high. Without merging these processes, you wouldn't have access to vital data that could lead to further investigations and the introduction of new controls to lower the incidents and reduce the risk.

5 Reduced Incident Rates

The automated confluence of risk management and incident reporting also ensures risks are managed with the appropriate controls – such as a regular check, a new policy or procedure, or a new piece of equipment to reduce the risk. Consequently, lowering the risk with controls will also reduce the likelihood of any associated incidents. With risk and incident data collected via standardised processes, firms can use precise reporting metrics to inform key decisions around the implementation of controls to prevent or mitigate high-priority risks or recurring incidents.

6 Enhanced Budgeting & Resource Allocation

Your business will have a finite budget available to manage risk and resolve incidents, making it essential to mitigate the highest priority risks and the most critical incidents from a financial, as well as an operational perspective. The data produced by an integrated risk and incident solution can be used to accurately gauge resource allocation based on likelihood and impact, allowing you to channel your budget and manpower where it's needed most.

7 Improved Collaboration & Cross Functional Data Sharing

GRC software breaks down entrenched barriers to managing risk and incident reporting in unison, such as manual processes, disparate systems, siloed teams and cultural resistance. Data capture inconsistencies and communication bottlenecks that hinder data sharing are replaced by efficient workflows and automated processes – enhancing collaboration across teams. This ability to transform risk management and incident reporting from fractured independent processes into an integrated discipline that's underpinned by seamless data sharing and precise mapping offers your business a strategic advantage: you can easily identify important linkages between risks and incidents and manage them via a central point of oversight.

8 API Integrations with Other Systems

GRC platforms can also integrate with other enterprise systems, like HR systems and cybersecurity ticketing tools, to automatically log relevant data when an incident occurs and link it to compliance obligations & risks – reducing manual entry and providing accuracy. This seamless integration allows for real-time data updates and cross-referencing, ensuring that incident logs are current and reflect the latest information.

9 Enhanced Regulatory Compliance

Many modern regulations have clear mandates about resolving incidents quickly to minimise disruptions and having sufficient controls in place to effectively manage operational risk. Opting for a GRC platform that can integrate risk management and incident reporting can support compliance with a variety of standards and regulations – enabling firms to demonstrate best-practice risk management processes and prove that they are proactively resolving incidents – supporting regulatory compliance efforts.

10 Integrated Reporting Outputs

Managing risk and incidents in one centralised platform brings a wealth of combined reporting outputs. This enables your business to generate the insights needed to create meaningful metrics that drive informed risk-related decision-making - helping to reduce risk levels and incident rates. Report on incident rates and examine the root causes to identify gaps in your risk register, understand what risks have turned into full-blown incidents, and monitor control effectiveness by analysing risk and incident data. Software provides robust reporting tools that allow your business to analyse incident trends and identify escalation bottlenecks, the information can be subsequently used to guide risk management efforts.

Conclusion

Integrating risk management and incident reporting into a single Governance, Risk, and Compliance (GRC) platform is essential for organisations seeking to enhance their ability to manage risks and respond to incidents effectively. By consolidating these functions, companies can seamlessly capture and analyse data from incidents, which often serve as indicators of underlying risks. This integrated approach allows for the identification of process gaps, system failures, and other vulnerabilities, enabling the implementation of controls to prevent future incidents. It also fosters a proactive approach, where the insights gained from incident data inform risk management strategies, ultimately reducing the occurrence of incidents and improving overall organisational resilience.

Using a GRC platform to automate and align risk management with incident reporting streamlines processes, reduces human error, and ensures real-time data accessibility for all stakeholders. This not only enhances collaboration across departments but also supports compliance with regulatory requirements by providing a transparent, audit-ready record of risk and incident management activities. The integrated system also facilitates better resource allocation by prioritising risks and incidents based on their potential impact, thereby optimising both financial and operational outcomes. A unified GRC platform empowers businesses to transform fragmented processes into a cohesive strategy that drives informed decision-making, lowers risk levels, and improves incident response times.

About Camms, a Riskonnect Company

Camms, a Riskonnect Company offers powerful GRC software that offers best-practice risk management and incident reporting in one unified platform alongside a whole host of other governance, risk and compliance capabilities.

Key capabilities include:

Risk Management

Establish a digital risk register and roll out risk assessments & control checks online - with all data feeding into the platform. Set up a control framework to successfully reduce unwanted risk. Monitor risk levels against KRI's and your risk appetite. Use automated workflows to escalate risk and implement risk treatment actions. Access dashboards & reports to understand key actions and provide a holistic view of risk. Link risk to your strategic objectives to achieve your goals.

Incident Management

Report incidents, hazards, near misses, and emerging risks via online incident forms that feed directly into the platform. Use automated workflows to conduct investigations, determine impact, perform root cause analysis, and monitor cases until closed. Use reports & dashboards to spot trends and introduce controls to reduce reoccurrence and link incidents back to the originating risks.

Third Party Risk Management

Build an online library of all your vendors - capturing critical details regarding contract, pricing, SLAs, and KPIs. Monitor supplier performance. Formalise the onboarding and offboarding process. Use Benchmarking and scorecards to rate and select vendors and understand any potential threats.

Business Continuity Planning

Identify business critical processes and build a business process register. Create best-practice BCM plans linked to each critical business process and conduct regular Business Impact Assessments (BIAs). Perform business process modelling and carry out scenario and vulnerability testing. Activate BCM plans based on incidents logged and track recovery progression.

Compliance

Build a comprehensive obligations library of relevant regulations, legislation, policies, and internal procedures and monitor compliance. Implement a best-practice regulatory change management workflow. Receive notification of upcoming regulatory changes from your preferred content provider. Implement a best-practice policy management process. Introduce best-practice compliance processes for conflicts of interest, sanctions checks, bribery & corruption, anti-money laundering, disclosures, whistleblowing, gifts & hospitality, and feedback & complaints.

Audits & Inspections

Schedule and manage internal and external audits. Formalise the results and use automated workflows to implement the required actions. The platform provides a complete history of all your audits and their findings and any outstanding actions or compliance failures.

Cyber & IT Risk Management

Build a cyber risk register, monitor cyber risk, and implement the relevant controls. Access frameworks to ensure compliance with data privacy regulations like ISO 27001, GDPR & NIST. Manage & resolve cyber incidents and maintain a cyber asset register.

ESG

Plan out an environmental, social and governance (ESG) strategy and monitor progress. Manage ESG related risks, incidents, and compliance obligations. Confidently report on the progress of key metrics and ESG initiatives.

Workplace Health & Safety

Maintain workplace health & safety registers, identify & address hazards, and create & track actions to resolve issues. Staff can report incidents, log hazards & near misses, and carry out safety checks via the mobile app.

Benefits include:

Highly configurable

Automated workflows & alerts

Enhanced collaboration

Clear insights to support decisions

API Integrations

Effortless reporting

Better visibility

Integrated GRC

RISK MANAGEMENT
INCIDENT MANAGEMENT