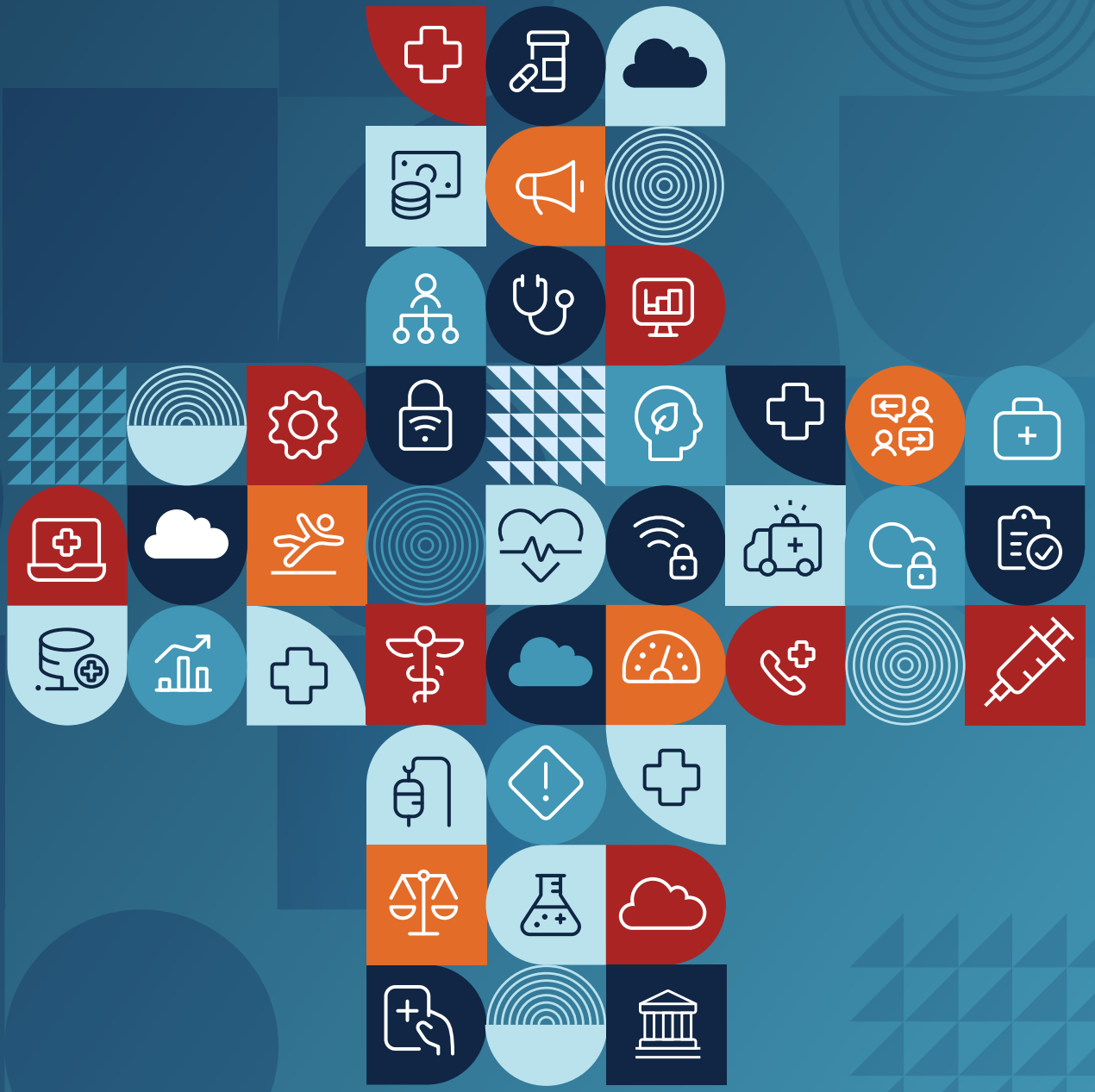
Automating Governance, Risk, and Compliance in Healthcare:

Safeguarding Care and Building Trust



riskonnect

In a highly regulated industry like healthcare, which is strewn with operational risk and experiences a high number of incidents, having strong Governance, Risk, and Compliance (GRC) processes to protect the organization and safeguard patient safety is vital. Healthcare data is also a goldmine for cybercriminals, making IT GRC equally as important in protecting sensitive data and maintaining patient trust.

Patients place their well-being in the hands of medical professionals and the institutions they work for, expecting the highest standards of care and the utmost protection of their sensitive data. However, behind the scenes, a complex web of regulations, ever-evolving threats, ethical considerations, risks, and compliance demands can negatively impact patient safety and confidentiality if not managed correctly.

This eBook will explain how to:

- **Enhance Patient Safety and Maintain Operations:**
  By minimising operational risks.
- **Ensure Regulatory Compliance:**
  By implementing workflows to streamline compliance monitoring.
- **Promote Ethical Conduct:**
  By fostering a compliant, transparent, and accountable culture.
- **Protect Patient Safety:**
  By reducing risks and incident rates.
- **Safeguard Critical Patient Data:**
  By managing cyber risks and incidents and operating in line with data privacy regulations.

Discover how your organization can achieve better patient outcomes, improve operational efficiency, and gain a stronger competitive edge.

Which areas of GRC are important in healthcare?

For healthcare organizations, GRC encompasses a vast array of critical areas:

1

Risk Management

This involves identifying, assessing, and mitigating potential risks to patient safety and operational efficiency. From operational risks, downtime, outages, and equipment failure, to strategic and compliance related risks, healthcare organizations have a lot to contend with. A robust risk management strategy and effective controls are crucial to identify, assess, and mitigate these risks before they disrupt operations or harm patients.

2

IT and Cyber GRC

Many healthcare organizations rely on a wide variety of systems and applications to keep their operations running, storing vast amounts of sensitive patient data, which makes cyber security and data privacy a key priority. Healthcare organizations must manage and mitigate cyber risk, resolve cyber incidents, ensure compliance with data privacy regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPPA), have sufficient business continuity plans in place, and build a strategy that ensures their IT infrastructure is fit for the future.

3

Third-Party Risk Management

Healthcare organizations deal with a variety of third parties, suppliers, and contractors, all of which can cause risk to the organization. Therefore, third-party risk management is essential to understand potential threats and keep a close eye on supplier performance.

4

Incident Management

Swift and effective response to incidents like data breaches , accidents, and incidents, and system downtime is vital. A clear incident response plan minimizes disruption, protects patient privacy, and ensures incidents are resolved quickly.

5

Compliance and Audit

The healthcare sector is highly regulated by national, federal, and state regulations. Examples of these include HIPAA to safeguard patient privacy, the Health Information Technology for Economic and Clinical Health Act (HITECH) to protect electronic health data, the Stark Law and the False Claims Act (FCA). The Care Quality Commission (CQC) is the main regulator in the UK. Failure to comply can result in hefty fines, reputational damage, and even suspension of operations. Healthcare organizations are also regularly audited to ensure compliance with various regulations and standards, as well as carrying out their own internal audits to improve patient safety. All of this must be documented, ensuring outcomes are captured and addressed.

6 Conflicts of Interest

Maintaining patient trust requires vigilant management of conflicts of interest. Financial ties between healthcare providers and pharmaceutical companies, for example, must be transparent to avoid undue influence on patient care decisions. Firms must establish a clear due diligence process to detect conflicts of interest and establish a clear process for potential conflicts to be reported.

7 Sanctions Checks

Healthcare organizations must screen patients, vendors, and staff against government sanctions lists to avoid violations. Failure to do so can result in hefty fines and reputational damage. This involves keeping a clear list of sanctioned entities and performing documented due diligence checks for new contracts.

8 Anti-Money Laundering (AML)

Healthcare organizations are, by nature, susceptible to money laundering schemes. Therefore, implementing a robust AML program helps to detect and prevent suspicious activity. This involves performing regular due diligence checks on transactions and setting controls and checks to detect fraudulent activity.

9 Disclosures & Whistleblowing

Organizations must have clear channels for employees to report suspected fraud, misconduct, or violations. Fostering a culture of open communication encourages whistleblowing and helps to identify and address issues before they escalate. Many companies choose to implement discreet online reporting portals to facilitate anonymous reporting.

10 Gifts and Hospitality

Hospital executives hold huge buying power and are often susceptible to bribes in the form of gifts and corporate hospitality. Monitoring the giving and receiving of corporate gifts is essential to ensure alignment with policies and prevent bribery. Therefore, implementing a strict corporate gifting policy, monitoring gift giving, and setting thresholds is essential.

The Cost of Inadequate GRC Processes: Real-World Consequences

The stakes for ineffective GRC are high. Consider the following headlines:

Fines

Massachusetts General Brigham (2022)

This prestigious healthcare system agreed to a settlement of $1.6 million with the Department of Health and Human Services (HHS) for violating HIPAA regulations. The investigation revealed unauthorized access to protected patient health information (PHI) by unauthorised users.

Integris Health (2021)

The Oklahoma-based healthcare system agreed to pay $6.8 million to settle allegations of violating the False Claims Act (FCA). The investigation uncovered improper billing practices related to Medicare Advantage patients, highlighting the importance of accurate coding and billing compliance.

LabCorp (2020)

A leading laboratory chain agreed to pay $14.5 million to resolve allegations of failing to report suspicious activity related to potential healthcare fraud. This case underscores the responsibility healthcare providers have in identifying and reporting potential fraud schemes.

Data Breaches

Viverant PT (April 2024)

A ransomware attack affected Viverant PT, a physical therapy provider, compromising the data of over 6,500 patients. This incident showcases the increasing targeting of smaller healthcare organizations by cybercriminals.

Kaiser Permanente (August 2023)

A cyberattack compromised the personal information of over 13.4 million Kaiser Permanente members. The attackers gained access through a single compromised employee login, highlighting the importance of robust access controls.

Tricare Data Breach (2022)

Tricare, a healthcare program for the US military, experienced a breach when backup tapes containing electronic health records were stolen from a car. While the ability of the criminals to access the data is unclear, the incident was treated as a major data breach.

Shields Healthcare Group (March 2022)

An unknown attacker accessed Shields Healthcare Group's network server for two weeks, potentially compromising the data of an unknown number of patients. This incident emphasizes the need for continuous monitoring and rapid response to security threats.

The Pitfalls of Manual GRC: Why Automation Is Essential in Healthcare

The healthcare industry thrives on meticulous record-keeping, clear communication, and unwavering adherence to regulations. However, many institutions still rely on manual GRC processes, creating a minefield of inefficiencies and vulnerabilities.

Let's delve into the key problems plaguing manual GRC processes in healthcare and explore how they can hinder an organization's ability to deliver exceptional care.

1 Silos of Information and Inconsistent Practices:

Manual GRC processes often result in silos. Policies and procedures reside in paper documents or disparate digital formats, making it challenging to maintain a single source of truth. This inconsistency can lead to confusion and errors, as healthcare professionals struggle to locate the most up-to-date information. For instance, a hospital with a manual conflict-of-interest process might have different interpretations across departments, potentially leading to missed disclosures or ethical lapses. Siloed data makes it hard to map risks to any associated controls, incidents, or compliance obligations, making it hard to understand the impact of risk on operational performance.

2 Time-Consuming Workflows and Human Error:

Manual GRC processes are often tedious and time-consuming. Compliance officers and risk managers spend hours sifting through paperwork, conducting manual reviews, and updating spreadsheets. This not only reduces their capacity for strategic initiatives but also increases the risk of human error. Imagine a healthcare system manually tracking thousands of vendor contracts for potential conflicts of interest or manually checking risk assessment data to monitor risk levels. Inevitably, some details might slip through the cracks, exposing the organization to unnecessary risk.

3 Limited Visibility and Difficulty with Reporting:

Manual GRC often lacks real-time visibility into potential risks and areas of non-compliance. Identifying trends and proactively mitigating risk becomes a major challenge. For example, a healthcare organization struggling with a manual incident reporting process without automated reports, dashboards, and notifications might not become aware of recurring problems due to a lack of reporting outputs. This reactive approach can have devastating consequences.

4 Difficulty with Scalability and Regulatory Burden:

The healthcare landscape is constantly evolving, with new regulations and compliance requirements emerging regularly. Manually adapting policies and procedures to meet these changes is a cumbersome and error-prone process. A growing healthcare system with manual GRC processes might struggle to keep pace with the expanding regulatory burden, hindering its ability to operate efficiently and compliantly.

The consequences of ineffective GRC processes extend beyond wasted time and frustrated staff. Compliance failures can result in hefty fines, reputational damage, and even legal repercussions. Furthermore, inadequate risk management can lead to patient safety incidents and operational disruptions. By transitioning to an automated GRC solution, healthcare institutions can streamline processes, improve visibility, and ensure they are well-positioned to deliver exceptional care while ensuring compliance with ever-changing regulatory requirements.

The Automation Imperative:
Why Healthcare Needs Streamlined GRC

Manual GRC processes are becoming increasingly insufficient to meet the growing demands of the healthcare sector, which is why GRC software is becoming increasingly popular in this industry.

GRC software automates tasks, enhancing operational efficiency and improving data accuracy. These solutions offer proactive risk management, automated compliance, best-practice incident reporting, and streamlined audits, reducing risk and compliance costs, and freeing up valuable time for healthcare professionals to focus on patient care.

The healthcare sector faces a unique variety of pressures due to evolving regulations, demanding patient privacy laws, and the need for operational efficiency to deliver high-quality patient care. Traditionally, healthcare organizations have relied on manual GRC processes, but these manual approaches are proving increasingly inadequate in the face of today's challenges. Consequently, healthcare institutions are rapidly embracing automation and streamlining their GRC efforts to enhance efficiency and resource optimization. Oline GRC platforms enable them to improve accuracy and data integrity, achieve real-time visibility and proactive risk management, and streamline audits - all while reducing compliance costs.

Manual GRC tasks, such as policy maintenance, risk assessments, and incident reporting, are often repetitive and time-consuming. Automation streamlines these processes, freeing up valuable time for healthcare professionals to focus on what matters most - patient care. Automating data capture and reporting reduces the administrative burden on compliance and risk management teams, allowing them to dedicate their expertise to analyzing risk and compliance data and making improvements.

Moreover, manual data entry and verification are prone to human error, leading to inconsistencies and inaccuracies in GRC data. Data governance guidelines within GRC software, like mandatory fields, dropdowns, and searchable menus, minimize these errors, ensuring data integrity across the entire GRC process. Reliable and consistent data is crucial for effective risk management and compliance. Automation facilitates the collection, analysis, and visualization of data, providing a clear picture of the organization's risk landscape and enabling data-driven decision-making.

Manual processes often make it difficult to gain real-time insights into potential risks. Automated GRC solutions provide a holistic view of the organization's risk profile, allowing for proactive mitigation strategies and early intervention. Automated systems can continuously monitor key risk indicators (KRIs) and identify emerging threats before they escalate into major issues. This enables proactive risk management and helps healthcare organizations build resilience.

Furthermore, new healthcare regulations and standards emerge regularly, and manual GRC processes make it difficult to demonstrate how and when changes were implemented. Automated solutions provide live regulatory updates from third-party content providers that can easily be linked to relevant policies, processes, and procedures, making it simple to implement changes and keep an audit trail of events. Automation ensures consistent application of policies and procedures across diverse healthcare organizations, facilitating efficient implementation of new regulations and streamlining internal processes and policies in accordance with changing requirements.

Automated GRC solutions offer best practice audit management capabilities, making it easy to plan and schedule audits, capture findings, and implement remediating actions. This simplifies and streamlines the audit process, reducing preparation time and costs. Automation helps ensure consistent adherence to regulations, minimizing the risk of non-compliance, penalties, and reputational damage. Streamlining and automating GRC processes is no longer a luxury but a necessity for healthcare organizations. By leveraging automation, healthcare institutions can achieve greater efficiency, improve data accuracy, and gain real-time insights into their risk landscape and compliance status. Ultimately, this translates to better patient care, improved compliance, better decision-making, and reduced operational costs, allowing healthcare providers to focus on what truly matters: delivering exceptional healthcare services.

10 key GRC functions that can be automated through GRC technology

The healthcare sector generally balances delivering high-quality care while adhering to numerous regulations, abiding with ethical standards, and managing risks. Handling these areas manually can be time-consuming and prone to errors. Here we explain how GRC software helps healthcare institutions automate ten key areas critical for maintaining strong compliance and a risk-regulated operation.

1 Risk Management

2 IT and Cyber GRC

3 Third-Party Risk Management

4 Incident Management

5 Compliance and Audit

6 Conflicts of Interest

7 Sanctions Checks

8 Anti-Money Laundering (AML)

9 Disclosures and Whistleblowing

10 Gifts and Hospitality

riskonnect.

1

Risk Management

The healthcare sector faces numerous risks, from patient safety concerns to operational failures. Managing these risks manually is often inefficient, hindering proactive strategies. GRC software automates risk management by providing a framework to identify, assess, and mitigate risks more effectively.

The software offers a centralized risk register, allowing healthcare institutions to establish an online, searchable database, where departments can log potential risks, categorize them by type, and assign severity ratings using a predefined framework. This centralized approach ensures a comprehensive view of all risks across the organization.

Online automated risk assessments improve the risk assessment process, as teams can complete risk assessments, questionnaires, and surveys using online forms that feed directly into the platform. This makes it easy to collect consistent risk data from various departments, building an accurate view of risk exposure. Automated workflows further streamline this process by sending out forms regularly to remind staff to complete them.

Risk monitoring is another critical aspect of GRC automation. Teams can define KRIs for each risk and implement automated monitoring to track risk levels. They can use the data to calculate the likelihood and impact of risks and analyze data from assessments and surveys. API integrations with internal systems and data sources pull operational data from other systems and spreadsheets into the risk platform, allowing for continuous assessment and early identification of emerging threats based on live operational data. This proactive monitoring helps prioritize risks and implement appropriate mitigation strategies. Teams can also use KRIs to define a risk appetite and operate within it.

Automated workflows streamline the risk management process by assigning ownership of identified risks, escalating high-priority risks to management, and tracking the progress of mitigation efforts, control checks, and testing.

Teams can build a control library within the platform, and set controls to mitigate risks. To ensure these controls are effective, teams can automate control checks and control testing with everything documented in the platform so it can be easily reported on.

The dashboards and instant reports provided by the GRC software offer personalized, user-friendly interfaces for staff at all levels to complete risk-related tasks online. Operational staff can view their tasks, managers can monitor risks and task completion in their areas, and senior leaders can get a holistic view of risk across the enterprise. Automated reporting tools offer real-time insights into the organization's risk profile. Teams can view heat maps, risk register summaries, bow-tie visualizations, and even Microsoft Power BI reports, enabling data-driven decision-making for effective risk management strategies.

Teams can use the data in the GRC software platform to support continuous improvement and growth opportunities by analyzing historical risk data to identify trends and patterns. This proactive approach allows healthcare institutions to address recurring risks and implement preventive measures and controls.

GRC platforms align risk management processes with industry best practices and strategic objectives, ensuring that healthcare institutions can take calculated risks that improve performance and contribute to achieving their goals, while mitigating those that could negatively impact their strategic aims. By using GRC software to align risk management processes with industry standards, such as ISO 31000, institutions can build a more resilient and proactive risk management program, ultimately improving patient safety, operational efficiency, financial stability, and long-term sustainability.

By automating risk management with GRC software, healthcare organizations can proactively identify and mitigate risks before they escalate into major incidents, improve data-driven decision-making, free up resources for analysis and strategic initiatives, enhance staff engagement, and foster a culture of risk awareness.

2

IT and Cyber GRC

Healthcare providers manage vast amounts of sensitive personal data and depend on numerous systems and applications to maintain operations – this makes IT GRC a critical aspect within the healthcare sector.

GRC software can support firms with IT and cyber GRC. Teams can use the software to build an online cyber risk register, where risks are categorized and rated based on their likelihood and impact. Cyber risk assessments are conducted using online forms, with all data feeding into the platform. Automated workflows distribute these forms to relevant stakeholders, chase incomplete information, and alert stakeholders about high-risk areas that need attention.

Ensuring compliance with data privacy regulations like HIPAA, ISO 27001, and GDPR is another critical area where GRC automation excels. The platform provides best-practice templates and forms to structure operations in line with these cybersecurity regulations and ISO standards. Automated workflows monitor compliance, escalate issues, and enable teams to implement corrective actions as needed.

Asset management can also be streamlined using a GRC platform. Teams can maintain an up-to-date asset management library in the tool. Reports on aging equipment and license expiry dates can be easily generated, allowing for effective budget management and ensuring all IT equipment meets the latest data privacy and IT security requirements.

For IT and cyber policy management, the GRC platform is invaluable. Teams can maintain an active library of IT current policies and monitor expiry and revision dates. Workflows automate the entire policy lifecycle, from creation and approvals to signoffs and attestations, keeping a fully documented log of all policies and their revision histories.

Cyber audits can also be managed efficiently using GRC software. Teams can create templates for both internal and external audits, creating fields for each aspect of the audit. Teams complete online forms to capture audit findings, and automated workflows support the implementation of corrective actions, ensuring the audit process is fully documented and transparent. Similar audits can easily be duplicated to reduce administrative work.

Business continuity planning is another area where GRC automation software proves essential. Critical processes are identified, and a business process register is built on the platform. Business continuity management plans are created for each process and business impact assessments (BIAs) are conducted. Business process modelling helps firms to understand the impact if a critical process fails, and firms can align business continuity management (BCM) plans with recovery time objectives (RTOs). BCM plans can be instigated based on incidents logged, with the status of these plans readily viewable as the plan progresses. Disaster recovery and vulnerability testing can also be carried out in the platform to identify and address gaps in the process.

With automated IT GRC software, healthcare organizations can proactively manage risks, ensure compliance, streamline asset management, and maintain comprehensive business continuity plans. This not only enhances operational efficiency but also strengthens the overall security posture of the organization, safeguarding sensitive data and maintaining trust in healthcare services.

3

Third-Party Risk Management

The healthcare sector depends on a complex network of third-party vendors, partners, and contractors, including medical device manufacturers, pharmaceutical companies, IT service providers, and billing processors. Managing the risks associated with these relationships is crucial for ensuring patient safety, data security, and operational resilience. Traditional, manual third-party risk management processes can be cumbersome and lack visibility, exposing healthcare organizations to unforeseen risks.

GRC solutions centralize vendor management and streamline the onboarding process, with online forms to capture essential information, such as contract details, costs, key contacts, service-level agreements (SLAs), and key performance indicators (KPIs), building a comprehensive vendor register. Vendor risk assessments are standardized and administered electronically through an online vendor portal, ensuring consistent data collection and facilitating risk scoring based on predefined criteria. This data-driven approach provides valuable insights for decision-makers, allowing them to compare vendors, identify potential risks and make informed choices regarding vendor selection and contract negotiations.

Continuous monitoring is another significant advantage of managing third party risk using a GRC platform. The tool can integrate with various data sources, including billing systems, inventory management systems, and IT security platforms, to automatically monitor vendor performance against SLAs and KPIs. Real-time alerts are triggered when deviations are detected, enabling proactive risk identification and addressing potential issues before they escalate into significant disruptions or security breaches. The GRC platform also enhances communication and collaboration by establishing automated workflows to track corrective actions and ensure timely resolution of performance issues.

Moreover, GRC platforms can monitor external data sources, such as news articles and regulatory databases, to identify emerging risks associated with existing vendors. This proactive monitoring allows healthcare institutions to address potential risks before they impact patient care or data security. The centralized repository within the GRC platform stores all vendor-related information, including contracts, risk assessments, performance data, and communication records, providing a holistic view of the entire third-party ecosystem. Every interaction and activity within the platform is automatically documented and time-stamped, creating a comprehensive profile of each vendor and the potential risks they pose.

Automated reports and dashboards offer real-time insights into the overall performance and risk profile of the third-party vendor network, empowering healthcare leadership to make strategic decisions regarding vendor relationships and resource allocation. This data-driven approach ensures that healthcare institutions can demonstrate due diligence and implement effective risk mitigation strategies.

By leveraging GRC technology to automate third-party risk management, healthcare institutions can streamline vendor onboarding, conduct standardized risk assessments, continuously monitor vendor performance, and maintain auditable documentation.

4

Incident Reporting

In the healthcare sector, ensuring patient safety and keeping operations running is a top priority. However, even with the best risk management processes, incidents, hazards, and near misses will occur, so they must be managed and resolved quickly. When relying on traditional incident reporting processes, like spreadsheets and emails, timely investigations and corrective actions often take long periods of time.

Using a GRC software platform to implement automated incident reporting allows healthcare workers to log incidents via online forms or using a mobile app - anytime, anywhere. The digital nature of the platform allows staff to attach relevant evidence, such as photos, videos, and documents, facilitating a comprehensive understanding of the incident and its contributing factors.

Most GRC platforms also offer an anonymous reporting portal, enabling staff to report sensitive incidents or whistle blow without fear of repercussions, fostering a culture of transparency and providing a more complete picture of potential issues.

GRC technology also enables the configuration of automated workflows based on the type and severity of the reported incident. These workflows can trigger immediate notifications and escalate reports to relevant personnel, such as supervisors, risk management teams, and legal departments. The automated assignment of ownership and deadlines ensures timely investigation and resolution of reported incidents. The GRC platform facilitates communication and collaboration among team members, allowing for a coordinated response and faster resolution.

Using a GRC platform builds a comprehensive database of incident data. This facilitates the analysis of historical data, which can be used to identify trends and patterns, enabling healthcare institutions to implement targeted preventive measures and reduce the likelihood of similar incidents in the future. Management teams gain real-time access to incident reports and dashboards, allowing for informed decision-making regarding resource allocation, process improvements, and patient safety initiatives.

Automated incident reporting systems can be integrated with risk management modules within the GRC platform, allowing for the identification of specific risks associated with reported incidents. By analyzing the root causes of incidents, healthcare institutions can then identify potential weaknesses in their existing controls and use this information to strengthen control measures, preventing similar incidents from happening again.

Automated incident reporting also ensures consistency and standardization in incident documentation across the institution, facilitating compliance with regulatory reporting requirements. The GRC platform maintains a centralized audit trail of all reported incidents, investigations, and corrective actions, allowing healthcare institutions to demonstrate their commitment to patient safety and regulatory compliance during audits. This fosters a culture of continuous improvement within the organization.

By streamlining the incident reporting processes, facilitating data-driven analysis, and promoting a culture of safety, automated GRC solutions empower healthcare providers to prioritize patient well-being, mitigate risks, and ensure compliance with regulatory mandates.

5

Compliance and Audit

Manual compliance and audit processes are often time-consuming and inefficient, hindering proactive risk mitigation. GRC technology provides automation solutions that streamline compliance efforts and automate the auditing process, significantly enhancing operational efficiency and regulatory adherence.

Teams can build an online obligations register, building a library of all relevant regulations, legislation, and internal policies and procedures. Controls, step-by-step processes, and checks are implemented using automated workflows, templates, and forms to ensure compliance with each requirement across multiple jurisdictions.

GRC solutions have the ability to integrate with regulatory content providers and legal service providers to scan the horizon for regulatory changes, facilitating timely notifications to organizations about new compliance requirements. These regulatory changes are automatically linked to relevant internal policies and procedures, facilitating the identification and updating of policies and procedures to align with new regulations via a best-practice regulatory change management workflow, providing adequate proof of compliance.

Additionally, GRC software offers a framework for managing policy revisions, incorporating automated workflows for policy reviews, approvals, signoffs, and implementation, thus involving all stakeholders in the policy management process while maintaining a clear audit trail of any amendments. Automated workflows facilitate policy review and approval by designated personnel, fostering accountability and ensuring proper vetting before implementation. GRC systems can also track employee acknowledgment and attestation of compliance with specific policies, demonstrating employee awareness and commitment to compliance. Automated features manage the entire policy lifecycle, ensuring that staff always work with the latest versions of policies and procedures.

GRC solutions also enhance data privacy compliance and audit readiness. Healthcare organizations can access out-of-the-box templates to operate in line with key data privacy requirements like HIPAA, ISO 27001, and GDPR, with the system providing a complete audit trail of compliance.

Audit planning and execution are another key benefit of GRC technology. Teams can use the GRC platform to plan and schedule their upcoming internal and audits, creating a series of online forms to capture key findings. Automated workflows guide the audit process, assigning tasks, managing document requests, and facilitating communication between audit teams and relevant departments. The platform then captures and analyses audit findings, triggering workflows to assign and track corrective actions, ensuring timely remediation of identified deficiencies.

Overall, automated compliance and audit functionalities available in GRC platforms empower healthcare institutions to navigate the complexities of regulatory changes, manage internal policies effectively, and improve audit outcomes. This comprehensive approach minimizes compliance risks and improves audit readiness. Real-time dashboards and reports provide clear insights into the organization's compliance posture. Automated reporting tools provide actionable insights for corrective actions and continuous improvement of compliance efforts.

6

Conflicts of interest

Conflicts of interest in healthcare pose a significant risk to patient care and public trust. It's crucial for healthcare professionals to make decisions based solely on medical necessity and patient wellbeing, without personal or financial biases. GRC technology offers solutions to automate conflict of interest management, promoting ethical decision-making and ensuring transparency.

Teams use the platform to build profiles for each staff member, capturing critical information, including relevant personal and professional information, financial interests, vendor relationships, affiliations, and any other data that could influence decision-making. This database can then be used to perform checks for potential conflicts of interest.

GRC solutions also offer a centralized conflict declaration platform where healthcare staff can disclose potential conflicts of interest via a discreet online portal. Automated workflows route disclosures to the appropriate personnel for review, ensuring timely identification and mitigation of conflicts. GRC platforms can also incorporate pre-defined criteria to assess the severity of conflicts, prioritizing those with the highest potential impact on patient care.

Upon identifying a conflict of interest, the GRC platform facilitates the development and implementation of mitigation strategies. This might involve excluding the staff involved in the conflict from specific decisions or adjusting roles and responsibilities. Comprehensive documentation of all actions taken to manage conflicts ensures transparency and adherence to internal policies and regulatory requirements. Automated reporting tools provide insights into policy adherence, types of conflicts identified, and risk trends, empowering leaders to further refine their conflict-of-interest management strategies.

A culture of disclosure, coupled with automated conflict management checks, ensures compliance with regulations and ethical codes, fostering trust with patients and regulatory agencies. By mitigating conflicts of interest, healthcare institutions safeguard patient care, ensuring decisions are made solely based on medical necessity and patient wellbeing.

7

Sanctions Checks

Healthcare providers rely on a vast network of suppliers to deliver high-quality patient care, from medical equipment manufacturers to staffing agencies and contractors. However, they must also ensure ethical sourcing practices and avoid dealings with sanctioned entities. GRC technology offers solutions to automate sanctions checks, ensuring compliance with regulations and ethical standards.

Through a GRC solution, organizations can maintain a centralized repository housing an up-to-date sanctions list that also integrates with trusted providers for automatic updates. This real-time list management eliminates the risk of non-compliance due to outdated information. During supplier onboarding, automated sanctions checks, which screen supplier data against the sanctions list, are carried out, flagging potential matches for further investigation. This streamlined process allows for swift identification and mitigation of potential sanctions breaches.

Automated escalation workflows ensure timely intervention when potential sanctions matches are identified, preventing accidental dealings with sanctioned entities. A comprehensive audit trail of all sanctions screening activities is maintained, facilitating compliance reporting and demonstrating due diligence. GRC technology can also prompt periodic reviews of existing vendors against the sanctions list, ensuring continuous compliance and proactive risk management.

Comprehensive reports provided by GRC platforms highlight trends and potential areas for improvement in sanctions screening activities. This data-driven approach allows healthcare institutions to refine their sanctions compliance strategies.

8

Anti-Money Laundering

The healthcare industry is accustomed to complex financial transactions and large-scale procurement. However, this complexity also opens doors to money laundering. Criminals may exploit these intricate financial flows to launder illicit funds as legitimate healthcare expenses. Automated AML tools within GRC technology help healthcare institutions combat money laundering and protect their financial integrity.

GRC platforms streamline customer onboarding by automating customer due diligence processes. Online forms collect essential customer information for risk assessment, including ownership structures and source of funds. Automated risk scoring assigns benchmarking and scoring based on pre-defined criteria, prioritizing high-risk customers for enhanced due diligence. Continuous monitoring of customer activity allows institutions to address potential money laundering risks proactively.

Integration with financial systems via API integrations enables real-time monitoring of all financial transactions. GRC solutions use automated control monitoring to identify suspicious activity, such as unusual transaction patterns, and trigger automated alerts for investigation. The platform also streamlines the generation of Suspicious Activity Reports (SARs) required by regulatory bodies, ensuring timely and accurate reporting of potential money laundering activity.

A centralized repository within GRC platforms stores all AML-related data, providing an audit trail for regulators and ensuring easy access to relevant information for regulatory inquiries.

9

Disclosures and Whistleblowing

The healthcare sector is entrusted with ensuring patient safety and upholding ethical standards. To fulfil this duty, it is crucial to provide a safe and confidential avenue for staff and patients to report concerns regarding potential misconduct. GRC technology plays a vital role in automating these disclosure and whistleblowing processes, promoting a culture of transparency and accountability within healthcare institutions.

GRC solutions offer secure and anonymous reporting channels through dedicated online portals. These portals allow individuals to report concerns, such as medical malpractice, unethical supplier relationships, or harassment, without revealing their identities. Configurable anonymity settings cater to different comfort levels, ensuring that whistleblowers feel safe to report without fear of retribution.

Automated workflows within GRC platforms manage the escalation of reported concerns based on their nature. This ensures that critical issues are promptly addressed by the appropriate personnel, minimizing potential harm or disruption. The platforms also facilitate secure evidence management, allowing for the secure upload and storage of supporting evidence for each disclosure report.

Efficient case management is facilitated through automated workflows that track the progress of each reported case. This central repository allows designated personnel to monitor investigations, ensure timely resolution, and keep relevant stakeholders informed. Data-driven action planning based on automated reporting tools helps healthcare institutions identify systemic issues and take proactive measures to prevent recurring incidents.

GRC technology can be configured to integrate with internal policies and procedures regarding whistleblower protection, ensuring a zero-tolerance approach to retaliation against whistleblowers.

10

Gifts and Hospitality Management

Gifts and hospitality play a vital role in maintaining business relationships, but in healthcare, monitoring this is crucial to prevent bribery and corruption. GRC solutions automate this process by ensuring compliance and ethical conduct. User-friendly interfaces enable staff to log the giving and receiving of gifts, while automated workflows route requests for approval based on predefined criteria. Lower-value gifts can be set to automatically approve, while higher-value items can follow an escalation route for approval in alignment with company policy.

Automated threshold checking flags potential compliance concerns based on gift value, which can be customized for different roles or locations. Any suspicious activity is flagged for investigation and data analysis tools identify trends and risk areas. This data-driven approach allows targeted training initiatives for high-risk departments or individuals.

All disclosures, approvals, and communication related to gifts and hospitality are stored in the GRC platform, providing a complete audit trail for proof of policy compliance. Real-time dashboards provide leaders with insights, promoting proactive issue identification.

Automated gifts and hospitality management promotes consistent policy application and transparency, fostering an ethical culture. Prioritizing ethical conduct enhances the institution's reputation for integrity and responsible business practices.

Conclusion:

Empowering Healthcare Compliance with GRC Technology

The implementation of GRC technology is a crucial step for healthcare institutions looking to improve regulatory compliance, reduce risk and incidents, and safeguard sensitive patient data. GRC automation offers a proactive solution to streamline compliance efforts, mitigate risks and foster a culture of transparency and accountability. By automating critical processes such as regulatory change, risk management, data privacy, conflicts of interest management, sanctions checks, anti-money laundering activities, whistleblowing procedures, and gifts and hospitality disclosures, healthcare institutions can free up valuable resources and focus on strategic initiatives and process improvements.

The benefits of GRC technology extend beyond efficiency gains. They include enhanced risk management, improved ethical conduct, and public trust reinforcement. GRC technology empowers healthcare providers to deliver high-quality patient care with confidence, knowing they operate within a comprehensive, up-to-date, and ethical framework. In the healthcare sector, GRC technology is not just an option; it's a necessity.

By embracing GRC software, healthcare institutions can:

- Achieve a proactive and efficient approach to compliance, freeing up valuable resources for patient care.
- Mitigate risks and safeguard patient safety, staff wellbeing, and financial integrity.
- Foster a culture of ethical conduct and transparency, strengthening public trust.
- Enhance the overall effectiveness and efficiency of the healthcare system.

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific.

Visit riskonnect.com to learn more – or schedule a meeting with our experts here.

riskonnect.

CONNECT NOW →

INTEGRATED RISK MANAGEMENT SOLUTIONS:

INSURABLE RISK
- Risk Management Information System
- Claims Management
- Billing
- Policy Administration
- Health & Safety

ACTIVE RISK MANAGER

BUSINESS CONTINUITY & RESILIENCE
- Business Continuity Management
- Operational Resilience
- Emergency Notifications
- Crisis Management
- Threat Intelligence

GOVERNANCE, RISK & COMPLIANCE
- Enterprise Risk Management
- Third-party Risk Management
- Environmental, Social & Governance
- Compliance
- Internal Audit
- Internal Controls Management
- Policy Management
- Project Risk Management
- Technology Risk Management
- AI Governance
- Business Strategy

HEALTHCARE RISK & PATIENT SAFETY