Technical Paper

Infor Risk and Compliance for healthcare providers

Why use continuous monitoring to address governance, risk, and compliance challenges?

Few industries are more tightly regulated than healthcare. Regulations are more complex than ever, putting increasing pressure on health systems and top executives to assure compliance and good operational governance, while driving strong business performance and doing so without increasing headcount.

Beyond Sarbanes-Oxley compliance, building a resilient compliance management foundation can take a healthcare organization into driving operational effectiveness within the extended enterprise. Integrating the concept of access and transaction control monitoring within the broader concept of continuous monitoring can help hospitals integrate disparate governance, risk, and compliance (GRC) needs with relevant IT and financial governance concepts.

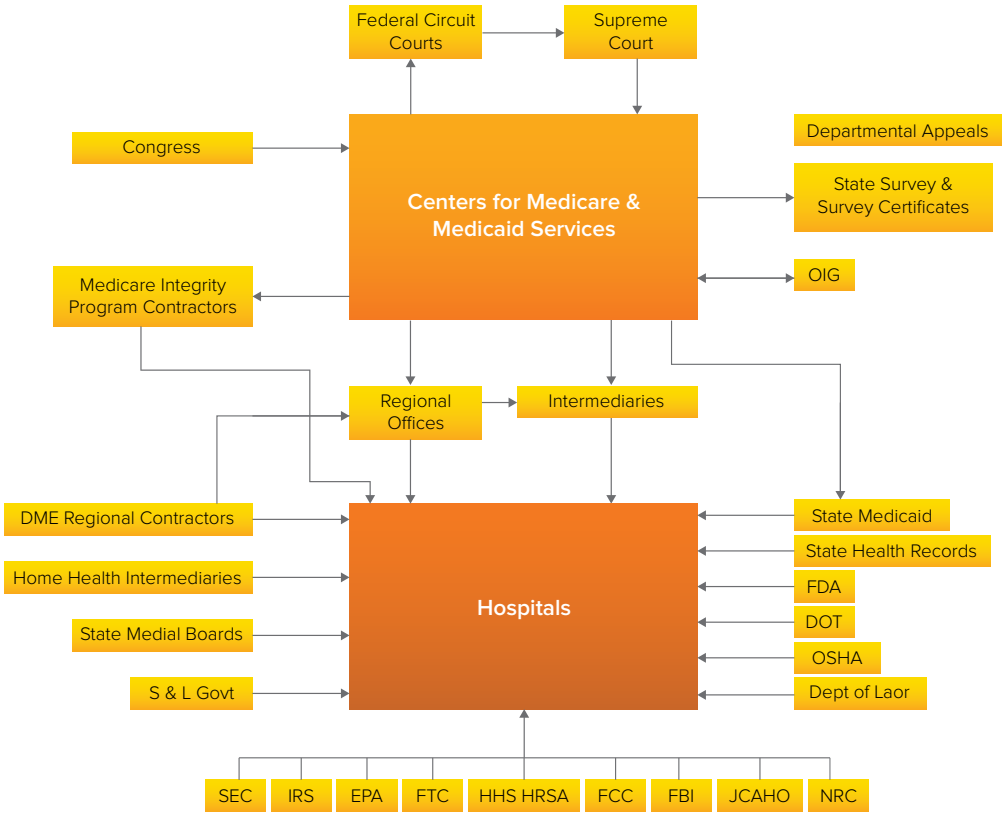
Financial results are no longer the sole basis of success. Fuelled by stakeholders' demands that healthcare organizations behave responsibly, new methods for measuring organizational health are emerging. Stakeholders now want evidence that hospitals and health systems are conducting operations efficiently and responsibly, encompassing their financial and compliance activities. Governance, risk, and compliance issues are hot topics today, thanks to many high-profile stories about health systems and other organizations that failed to meet regulatory requirements governing finance, compliance, patient privacy, and other areas. In each case, the leadership has increasingly been held accountable, capital funding has been negatively impacted, reputations have been tarnished, and communities have been left in doubt over the decisions and agendas of hospital officials.

One particular element of GRC that is a major concern for healthcare providers is access and transaction controls monitoring. Increasingly, leaders have come to understand that seemingly small operational control weaknesses can significantly impair operational performance. These obstacles might range from increased inventory that impacts costs, to over payments that decrease margins, to a leakage of confidential data that damages reputation and creates a compliance liability within the HIPAA framework.

Table of contents

Issues related to access and transaction control monitoring have become top priorities for health executives and compliance officials, thanks to highly publicized scandals and the release of several regulatory mandates designed to prevent issues ranging from fraud to compromised patient information.

The heathcare compliance challenge



The potential costs of noncompliance today are extremely high. A health system could face severe impact on brand, reputation, and valuation, in addition to the cost of litigation and remediation. Hospital executives cannot afford to only focus on regulatory compliance as mandated by Centers for Medicare and Medicaid Services (CMS) or other governing bodies. Ultimately, these areas are reported through the financial systems, and officials and leadership at the top can be held personally responsible for all compliance failures.

Here's a look at the typical IT and finance control monitoring pain points healthcare organizations face today.

Challenge	Impact to organization
Pervasive segregation of duties risk	• Difficult to effectively manage controls due to an array of mandates and interdependencies across business processes and IT systems • Lack of software that automates the process of analyzing and comparing controls, detecting potential risks, and providing the necessary information to IT and management
Costly, manual remediation results in greater chances of mistakes	• Highly inefficient, costly, and error-prone process of manually addressing compliance requirements, calling for extensive and costly testing • Manual risk and compliance activities trap related data within spreadsheets and other standalone documents, limiting visibility and monitoring of processes • Inadequate training of staff due to limited budgets
Uncontrolled role management and possibility of fraud	• Inability to achieve compliant role management that simplifies role definition and maintenance, providing a single source of truth • Defining role ownership at the business level rather than IT • Lack of unification across essential steps creating inefficient back-and-forth with security administrators
Inefficient and unauditable user provisioning	• Complicated manual mechanisms for ensuring compliant provisioning and staying fully compliant • Difficult to manually manage the user attestation process in back-office and clinical systems that is required by SOX 404 and HIPAA
Risk exposure: reactive vs. preventative approach	• High risk of negatively impacting brand and reputation, and incurring great costs if a reactive approach to compliance is chosen • Inability to cost-effectively monitor and deter fraud, waste, and abuse in financial systems • Difficult to minimize cash leakage that results from lack of accounting, such as payments received, vendor discounts not taken, and paying duplicate invoices

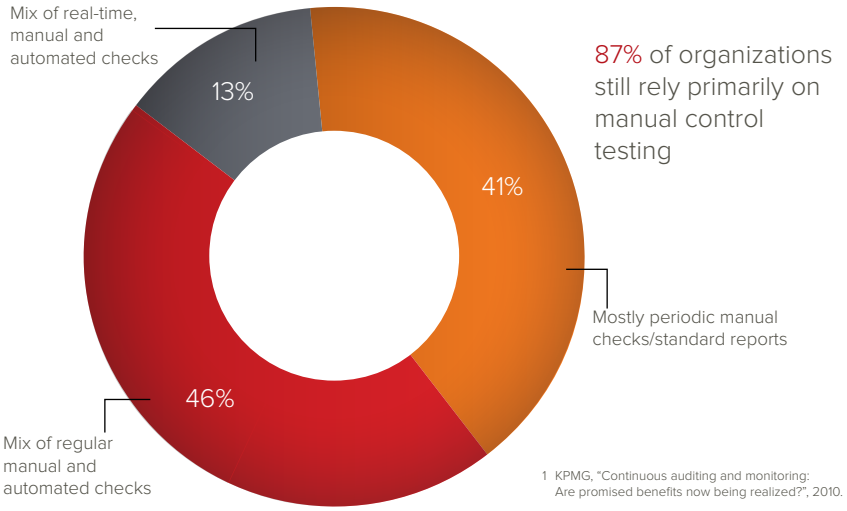
Why move to a single, integrated continuous monitoring platform?

With all the other emerging priorities, especially those associated with payments tied to Meaningful Use and quality of care, many healthcare organizations have responded to regulatory mandates by implementing a series of spreadsheet-based, disconnected, tactical, one-off projects to address a single regulation or organizational initiative. In 2010, KPMG conducted a study across all industries, and it's safe to say that healthcare can be counted in these numbers (see graphic). For healthcare providers, it is most often during their annual financial audit that compliance issues are raised and reported and the organization learns of impending risk.

Following is an actual summary of items a hospital was cited for in their annual audit—demonstrating the impact of a fragmented approach to addressing IT and Financial Control Monitoring:

1. Lack of segregation of duties—payroll.
2. Applicable payments from patients are not being collected upon completion of services or discharge.
3. No perpetual inventory system for pharmacy or central stores—just annual physical inventory.
4. Lack of financial oversight, balances not reviewed or adjusted properly in period closing.
5. Interim financial statements unreliable.
6. Capital asset capitalization policy does not comply with state requirements and is not consistently applied.
7. Payroll disbursement errors.
8. No written policies for the payroll process.
9. Inadequate controls over information systems.
10. Lack of segregation of duties regarding receipt of cash, posting, and writing off uncollectible accounts.
11. No review of billing rates entered into systems.
12. Affiliated hospital invoices not kept in the AP file.
13. Former employees do not have their computer access rights removed upon separation.
14. Patient medical records related to accounts receivable cannot be found.
15. Duplicate vendor payments and earned discounts not recovered.

What methods do you use to provide management assurance of your controls?[1]



87% of organizations still rely primarily on manual control testing

1 KPMG, "Continuous auditing and monitoring: Are promised benefits now being realized?", 2010.

As a result of these manual, disparate controls processes, several different kinds of fragmentation can result:

- Organizational fragmentation: A health system is accountable for good governance and compliance, not only within the confines of its own enterprise, but also across the extended enterprise. Disconnected, departmental activities used to identify and mitigate risk result in inconsistent policies, lack of transparency, and duplication of effort. As a health organization increases its collaboration with more partners, such as physicians or other local providers of care, the consequences of fragmentation intensify.
- System fragmentation: Governing principles and policies, risk measurement, and compliance with regulatory mandates are typically supported by departmental IT systems. Without centralized governance, systems may use different metrics, standards, and methodologies for analyzing risk and compliance information, making the aggregation of data a complex and time-consuming task. Local process optimization can further isolate communication.
- Regional fragmentation: Risks and policies are often defined and measured at the local level, without adequate consideration for their impact on the regional or enterprise mandates with which an organization must comply. Decision makers may overlook or be unaware of the interdependencies of various mandates and the risks associated with the multitude of jurisdictions in which they conduct business. Risks include noncompliance in specific markets.
- Growing number of isolated, fragmented GRC Initiatives: With the growing number of GRC initiatives, the problem of fragmentation becomes apparent. Horizontal mandates address such areas as financial reporting, security, privacy, records retention issues, and credit risk exposure that address all types of businesses. Vertical mandates address an exhaustive number of industry-specific areas.

Multiple levels of fragmentation, coupled with little investment in enterprise governance practices, compound the cost of addressing risk and managing compliance. Fragmented GRC activities may be the status quo, but they cost hospitals more than is necessary. A fragmented approach necessitates purchase and deployment of multiple GRC applications or manual methods for each process, followed by separate risk definition, policy setting, and compliance monitoring for each application. As a result, countless GRC policies, decisions, and data based on different metrics, standards, software, and methodologies need to be managed. The resulting complexity can make it impossible to aggregate information in order to gain a complete view of enterprise risk. Of even greater significance is the fact that fragmented efforts make it impossible to implement a cohesive GRC strategy for monitoring, identifying, and managing risk across the enterprise. This fragmentation, when replicated many times across different business applications and business functions, creates a GRC management nightmare. Each business process may have one or more different applications from which it is executed. And for each application, business and IT departments need to define risks, set policies, monitor compliance, manage attestations, address escalations and mitigations, generate reports, and more.

Without an integrated perspective on governance to guide risk profiling and mitigation, each problem would be solved in isolation. Clearly, a fragmented approach to GRC represents a massive and costly duplication of effort that impairs transparency and increases opportunities for weakness or issues to fall through the cracks until identified by a regulatory body. The key is to implement a single, holistic solution that works with all of the enterprise applications used to support business processes.

Top control challenges

- Segregation of duties
- Duplicate payments
- Employee reimbursements
- Unauthorized purchases
- Fraud prevention
- Overpayments
- Checks and approvals
- Compliance with policy
- Regulations
- Standardization

According to a KPMG survey	
Fraud detection/prevention	68%
ERM	50%
SOX 404	40%
Compliance	38%
Regulatory compliance	29%

Source: KPMG, Continuous Monitoring and Continuous Auditing survey, 2010.

What drives these challenges?

- Lack of staff
- Manual process
- Human errors
- Access to data
- Visibility to issues
- Mergers and acquisitions
- Decentralized operations
- Outsourcing

A single, holistic solution helps mitigate the following risks:

- Integration risk—Multiple disparate systems result in longer time to benefit, higher costs, and degraded performance due to interface conflicts. The risk is dependent on the extent and complexity of the systems and interfaces in question. Taking on the integration challenge in-house effectively transfers the risk from the vendor to the organization itself.
- Vendor-specific risk—Betting a critical piece of operation on a platform that is unlikely to be supported in the future or that is likely to be acquired by larger players greatly increases the risk of realizing any benefits from the implementation.

- Ongoing support risk—Supporting multiple systems over time from a number of vendors presents the challenge of software upgrades across many products and shifts the burden of support from the vendor to the customer.
- User adoption risk—Getting users acquainted with a single system with a common look and feel is less problematic than getting them to learn multiple systems with inconsistent procedures and terminology.

It is evident that implementing a single solution is an important step toward implementing a cohesive GRC strategy across the health enterprise. A true cross-enterprise continuous monitoring GRC solution delivers functionality across two dimensions:

- Breadth in terms of coverage of business processes, such as finance, supply chain, procurement, human resources, and IT.
- Depth in terms of seamless integration with multiple business applications, which may include software from a major vendor, as well as legacy and custom applications. In addition, all applications that are a part of the solution must feed to and from a single, centralized continuous monitoring GRC data repository.

Breadth and depth of cross-enterprise GRC help address a multitude of challenges and delivers benefits such as:

- Enterprise-wide risk tracking—Monitor risk across all enterprise applications and business functions by deploying a single solution rather than multiple applications that manage only a subset of control monitoring activities. This can significantly lower the effort and cost of GRC for an organization, freeing up resources for innovation and top-line growth.
- Greater transparency—Reduce missed opportunities and strategic misalignment through greater transparency into business operations across the health enterprise.
- Increased automation—Automate manual processes, which results in highly repeatable, consistent, and auditable processes. At the same time, automation enables fast, cost-effective reporting that saves time and money, and helps ensure that the data submitted to regulatory agencies is reliable.
- Greater flexibility—Quickly adjust to regulatory changes as per new legislation and market trends.

What can Infor Risk and Compliance deliver?

Infor® Risk and Compliance offers an automated approach for monitoring, identifying, and managing risk across the health enterprise application infrastructure. Continuous Monitoring provides an almost real-time snapshot of your IT and financial controls status, helping you reduce fraud, waste, and abuse.

Infor Risk and Compliance helps better align the functional areas of IT, finance, and internal audit and allows them to work more effectively as a team. Both IT and finance are able to work through their Infor-identified control violations in an easy-to-use and powerful workflow. Internal audit is able to handle an increased workload and perform their duties in a more consultative fashion, ensuring broader and more complete audit coverage.

Infor Risk and Compliance monitors controls, mitigate risks, and enforces governance policies for key business functions across multiple business applications. This holistic approach to GRC dramatically simplifies management and execution of controls monitoring activities.

A single monitoring solution that simplifies controls management and significantly lowers its costs. Whereas previously, a different application was required to manage each business process, with cross-enterprise Infor Risk and Compliance, only one is needed.

Visibility into controls risks and compliance across the enterprise. Having a single continuous monitoring solution means that risk definition and policy setting has to be done only once for the entire enterprise. It also means that metrics, standards, software, and methodologies for analyzing risk and compliance information are consistent across the enterprise, making it easy to aggregate data, gain a complete view of enterprise risk, effectively monitor compliance and risk, and adjust business processes to meet changing requirements, market trends, and regulatory mandates.

Monitoring of both IT and financial controls across the health enterprise. Within the IT controls area, Continuous Monitoring can be used for provisioning and on-going Segregation of Duties (SoD) management for many leading ERP systems, including those from Infor Lawson, Oracle®, and SAP®. The complexity and effort of manually conducting SoD is time-consuming, expensive, and mistake prone when using tools like spreadsheets, Word documents, and email. Infor Risk and Compliance easily connects to your ERP of choice, without affecting the performance of the transactions processed.

Optimized rules library for Segregation of Duties (SoD). Infor's complete Segregation of Duties (SoD) rules library has been enhanced through our large installed base and close working relationship with the leading audit firms. Our optimized rules library surfaces SoD violations quickly for review and remediation in our powerful and easy to use workflow. In addition, Infor Risk and Compliance seamlessly connects with your email system to involve users who may have no need to be connected to the solution on a regular basis. The solution maintains a complete audit trail of remediation activities, lowering the cost of internal and external audit reviews. Finally, the solution is easy for business users to learn and incorporates a large portfolio of reports and dashboards that are optimized for continuous monitoring.

Certification process for user attestation. Infor Risk and Compliance Certification Manager provides an automated approach for validating that individuals who have access to sensitive financial or personal information still need access. It's easy to use and requires minimal support.

Within the Certification Manager application, connections are made to any application where user attestation reviews need to be conducted. The Infor Risk and Compliance workflow can be adjusted to accommodate different hierarchies of review. In addition, all employee changes are captured by the system to reduce audit costs. This application can work with Microsoft® Shared Folders, Microsoft Active Directory, and a myriad of financial and clinical systems.

Governance of financial systems and processes. In this implementation, Infor Risk and Compliance can also be applied to the governance of financial systems and processes. In this implementation, the extraction of relevant financial information is automated and does not affect the performance of your ERP or financial application. Hundreds of out-of-the box rules have been develop to surface transactions, which
may include:

- Duplicate vendor payments
- Duplicate invoices
- Earned discounts not taken
- Suspicious or problematic posting to sensitive GL accounts
- Employee fraud
- Split purchase orders
- Excessive overtime
- Inventory discrepancies due to theft or unnecessary leakage
- Travel and expense abuses

The out-of-the-box rules delivered with Infor Risk and Compliance solution can be customized using our tools to extend the value proposition to other financial applications and systems. The solution workflow is easy to use, with all activity captured for later review by internal or external audit. In addition, the system operation is fully integrated into your installed email system for remediation activities.

Summary

While there are hurdles to adopting any GRC solution, Infor's unified approach and solution for continuous monitoring can greatly contribute to eliminating these challenges for health systems. It can lead to a reputation of accountability and responsibility by providing operational transparency and evidence of conducting business within ethical standards and regulatory mandates. Accountability is supported with a unified approach, predictive risk processes, integrated, continuous control monitoring, and lower costs for compliance.
A unified approach to continuous monitoring overcomes the challenges of driving hospital strategy, regulatory compliance, and risk management across disconnected systems, regions, and functions, creating increased business performance and organizational accountability. With accountability comes the ability to predict risks, as well as increased market value, stronger brand value, greater operational efficiency, and cost savings, and better strategic agility.

The Infor approach to continuous monitoring and our solution portfolio provides the framework and technology to help build a GRC architecture step-by-step, leveraging existing IT investments. Infor's business process expertise, industry knowledge, and global presence attract a continuously growing partner ecosystem that includes audit firms such as Ernst & Young, KPMG, PwC, and Deloitte. In combination, Infor and its partners deliver a comprehensive and integrated GRC solution portfolio unmatched by any single vendor in the market.

641 Avenue of the Americas
New York, NY 10011
800-260-2640
infor.com

About Infor

Infor is fundamentally changing the way information is published and consumed in the enterprise, helping 73,000 customers in more than 200 countries and territories improve operations, drive growth, and quickly adapt to changes in business demands. To learn more about Infor, please visit www.infor.com.

Disclaimer

This document reflects the direction Infor may take with regard to the specific product(s) described in this document, all of which is subject to change by Infor in its sole discretion, with or without notice to you. This document is not a commitment to you in any way and you should not rely on this document or any of its content in making any decision. Infor is not committing to develop or deliver any specified enhancement, upgrade, product or functionality, even if such is described in this document.

INFDTP1311384-EN-US-0615-2