August 2014

YALE NEW HAVEN HEALTH SYSTEM

Utilizing Technology to Enable GRC Across the Organization

CASE STUDY

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Yale New Haven Health System

Utilizing Technology to Enable GRC Across the Organization

Executive Summary

Historically, healthcare has approached governance, risk management, and compliance (GRC) from multiple directions, resulting in greater cost, redundancies, and risk. Over-reliance on documents, emails, and spreadsheets compounds complexity and cost as departments attempt to manage, scale, and report on GRC programs. Lapses are bound to occur as organizations struggle to keep pace with regulations, audits, and quality demands. Achieving prudent healthcare GRC requires defined processes, discoverable evidence, and the necessary technology architecture for managing and monitoring GRC across mandates. Yale New Haven Health System (YNHHS) achieved GRC with centralized visibility: the tools to monitor across departments and processes; the ability to collaborate across security, compliance, and hospital operations; a process for connecting dots between risk and compliance across the organization; and a way to integrate risk-based views to communicate "big picture" GRC. YNHHS found Modulo Risk Manager™, Modulo's GRC platform, met the core functionality requirements for IT GRC, privacy, and security compliance. Modulo Risk Manager has seen broad reception across YNHHS and has expanded beyond the initial IT GRC focus to include enterprise GRC applications.

Expanding Pressures in Healthcare

Healthcare, one of the most highly regulated and scrutinized industries, faces GRC trauma from every direction. Lapses are bound to occur as organizations struggle to keep pace with regulations, audits, and quality demands. As such, healthcare providers scramble to create effective GRC programs to address a breadth of risks, regulations, liability, and fines to which an increasing number of regulations expose them.

Many organizations, healthcare included, approach GRC from multiple directions, resulting in greater cost, redundancies, and risk. Departments that have no collaborative processes have no capacity to share GRC information. Over-reliance on documents, emails, and spreadsheets further compounds complexity and cost as departments attempt to manage, scale, and report on GRC programs. GRC projects then fail due to inefficacy.

Typically healthcare organizations face:

- A complex range of assessment and reporting requirements and an expensive approach to sporadic audits
- Increased risk, compliance obligations, fines, and exposure to legal liability as well as intensifying demands for compliance assurance across third-party business relationships

- No risk-prioritization of controls and requirements and a range of inconsistent expectations with respect to security; inconsistent definitions and monitoring of disparate requirements and corrective actions
- Challenges to efficiently reporting and communicating compliance across the organization and business units
- And, ultimately, low assuredness of adequately managed IT risk and security

The Bottom Line: A fragmented approach to risk and compliance management leads healthcare organizations to spend an unjustifiable level of money and effort meeting requirements, monitoring controls, performing assessments, and reporting. Increased scrutiny over healthcare compliance drives the need to streamline and fine-tune GRC management processes. Yet GRC for healthcare is no simple task: there are a variety of approaches, some add overhead cost and encumber processes while others enable operational efficiencies and improve security. Achieving prudent healthcare GRC requires defined processes, discoverable evidence, and the necessary technology architecture for managing and monitoring GRC across mandates.

Compliance Mandates Bear Down on Healthcare

- American Recovery and Reinvestment Act (ARRA)
- Cardholder Information Security Program (CISP)
- Centers for Medicare & Medicaid Services (CMS)
- Federal Information Security Management Act (FISMA)
- FTC Red Flag Rules
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Healthcare Information Technology Standards Panel (HITSP)
- The Joint Commission
- Medicaid Recovery Audit Contractor (RAC) Audits and Zone Program Integrity Contractors (ZPIC) Audits
- Office of the Inspector General Audits (OIG)
- Patient Safety and Quality Improvement Act (PSQIA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Stark Mandates
- State Mandatory Disclosure Laws

How Yale New Haven Health System Approached GRC

Yale New Haven Health System (YNHHS) achieved GRC with centralized visibility: the tools to monitor across departments and processes; the ability to collaborate across security, compliance, and hospital operations; a process for connecting dots between risk and compliance across the organization; and a way to integrate risk-based views to communicate "big picture" GRC. Best practice requires healthcare organizations to approach GRC management as related processes and controls, with these critical elements in mind. YNHHS accomplished this.

The Challenge Facing Yale New Haven Health System

YNHHS had historically approached GRC activities manually through different departments. They approached the array of GRC mandates with a bigger array of spreadsheets, documents, and email across inboxes, file-shares, and mountains of paper.

Consider the challenges…

- **On-premise assessments for over 300 remote sites.** Mandate requires physical on-premise inspections on privacy and security standards. A manual approach meant YNHHS could only assess about 10% of satellite locations per year.

- **Assessments for over 600 IT applications.** YNHHS's IT applications need to comply with HIPAA and other privacy standards due to sensitive protected health information (PHI) they store. A manual process limited assessments to 33% of their systems per year and could not scale due to in-house resource constraints and the exorbitant cost to outsource the project.

- **Manual approaches to a range of compliance mandates.** Compliance to HIPAA/HITECH, CT and NY Privacy and Security laws, JCAHO, Stark, Red Flag, FISMA, PCI DSS and other healthcare related oversight.

The Prescription to Their Problem

The health of YNHHS's GRC needed addressing before things grew out of control. The GRC team at YNHHS knew things had to change. In light of increasing risk and compliance pressures, they sought to create a sustainable process supported by technology architecture for GRC.

YNHHS went to request for proposal (RFP) to evaluate the top IT GRC solutions recognized by analyst firms. They narrowed the section from five to two and, of these, made a deeper analysis into cost and functionality.

YNHHS found Modulo Risk Manager™, Modulo's GRC platform, met the core functionality requirements for IT GRC, privacy, and security compliance projects across the organization's network of operations. Due in part to the company's willingness to negotiate, the solutions priced in at one quarter the cost of the other leading contender. The YNHHS team was further impressed with the knowledge and straightforward honesty of Modulo staff.

Consider the successes. . .

- **On-premise assessments for over 300 remote sites.** Where YNHHS previously performed assessments on 10% of off-site locations per year, they can now assess all 300+ sites. Using the Modulo Risk Manager Questionnaire mobile app streamlined site surveys on privacy and security requirements. The efficiency afforded by Modulo Risk Manager manifested in the ability to conduct individual on-premise site assessments in less than an hour with an additional fifteen minutes needed to finalize each assessment back at the main office. YNHHS management can view reports on the assessments in boardroom meetings presented directly from tablet devices.

- **Assessments for over 600 IT applications.** The YNHHS team completed all 600 IT application assessments in the course of a single year where previously they

could only get through a third of them. The fully automated application security assessment process in Modulo Risk Manager features standardized surveys and forms that are delivered in an intuitive and easy to use interface that has been well accepted by distributed groups across YNHHS. Findings from assessments are moved right into planned mitigation activities and tasks. YNHHS is able to identify and prioritize the most critical application security issues and track them through remediation.

- **Compliance to multiple standards.** YNHHS was impressed by the extensive knowledge base of regulations and frameworks within the Modulo Risk Manager system. They utilized this along with the system's flexibility to add the HITRUST CSF (Health Industry Trust Alliance Common Security Framework) and the system's ability to customize questionnaires and surveys to easily adapt the system to perform appropriate risk assessments for various business units and the enterprise.

YNHHS rapidly expanded their GRC implementation beyond the initial successful use cases for on-site and application assessments. The team found Modulo Risk Manager expanded well outside their initial IT GRC focus to include enterprise GRC applications. Modulo Risk Manager integrated platform currently manages the following projects for YNHHS's GRC program:

- Federal Information Security Management Act (FISMA) compliance and workflow
- Payment Card Industry Data Security Standard (PCI DSS) compliance
- Security and privacy program using the HITRUST framework, which is integrated into the Modulo Risk Manager content library
- Policy mapping
- Vendor and other 3rd party assessments
- Security design reviews
- Documentation, approval, and management of policy exceptions
- Management and filing of confidentiality requests, which everyone (employee and contractor) has to sign
- Assessments and regulatory compliance activities for fire, facilities, physical security, and health and safety
- Integration with other systems, including Rapid7 and Core Insight, to centralized and analyze data vis-à-vis GRC activities
- Audits around inappropriate access to patient records.

Modulo Risk Manager has seen broad reception across YNHHS and continues to expand into new areas. Other current areas of expansion include a pilot program to address the needs of the emergency preparedness group and two other GRC programs for the finance and internal control groups.

The Benefits of Using Modulo Risk Manager

Successful GRC delivers the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment with agility. GRC solutions should achieve better-performing processes and deliver reliable information on-demand. This enables a better-performing, less costly, and more flexible business environment.

YNHHS deployed Modulo Risk Manager, a GRC platform, with the following goals: understanding and managing risk, ensuring compliance with obligations, improving human and financial efficiencies, enhancing transparency, and managing GRC in the context of a dynamic and distributed healthcare environment.

GRC 20/20 measures the value of GRC engagement around the elements of efficiency, effectiveness and agility. Organizations need to be:

- **Effective.** At the end of the day GRC is about effectiveness — to ensure that the organization manages risk and compliance and is properly understood, monitored and managed at all levels of the organization. Effectiveness delivers a holistic understanding and prioritization of risk and compliance aligned with the business and kept under control. GRC effectiveness is validated through greater assurance of the design and operational effectiveness of controls to mitigate risk, achieve performance, protect integrity of the organization, and meet regulatory requirements.

    - **Modulo GRC is effective.** YNHHS has seen increased productivity in which they can complete more assessments in a given time period than they could before. Faster response time, better reporting, the ability to escalate issues, and the capability to follow through with full accountability in workflow and task management also key measures of efficacy. The accuracy of GRC information has also improved which increases effectiveness. Overall, YNHHS states that they have improved compliance and are better prepared for external audits and regulatory exams.

- **Efficient.** GRC solutions provide efficiency and savings in human and financial capital resources. Technology solutions that support business and GRC processes reduce operational costs by automating processes, particularly those that take a lot of time consolidating and reconciling information in order to manage and mitigate risk and meet compliance requirements. GRC efficiency is achieved when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations. GRC should reduce operational costs by providing access to the right information at

the right time, and reduce the time spent searching for answers.

- **Modulo GRC is efficient.** YNHHS has become more efficient in its use of resources allowing them to get more assessments done without increasing staff and even removing the overhead and dependency on external consultants. What had been time-consuming and manual processes are now automated through workflow and task management. YNHHS has moved from stacks of papers and lots of hours spent on assessments, with not much getting done in the process, to accomplishing everything in significantly reduced time. Where departments and individuals used to get multiple, often redundant assessments, they now receive one assessment to address a range of GRC areas.

- **Agile.** GRC solutions deliver business agility when organizations can respond rapidly to changes in the business environment (e.g., employees, business relationships, mergers and acquisitions, new laws and regulations) as well as the external environment (e.g. economic risk, new laws, and regulations) and communicate changes to employees. GRC agility is also measured in responsiveness to events and issues; organizations can identify and react quickly to incidents so that action can be taken.

  - **Modulo GRC is agile.** YNHHS operates in a very dynamic environment in which the organization is very distributed across over three hundred locations. The business, regulatory, and risk environments are in a constant state of change. Modulo Risk Manager has allowed the hospital to remove overlaps between groups and use a consistent information architecture that has enabled them to achieve agility across the organization. YNHHS has found Modulo Risk Manager flexible and adaptable to a range of business needs.

GRC 20/20's Final Perspective . . .

To reliably achieve objectives while addressing risk and compliance, healthcare organizations need to approach GRC management as related processes and controls. YNHHS accomplished this with the correct strategy, process, supporting information and technology architecture. Modulo Risk Manager quickly became the architecture backbone for enterprise GRC after showing rapid success within IT GRC in its ability to be used and adapted to a range of complex GRC needs across the organization.

About GRC 20/20

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com