



# HEALTHCARE ENTERPRISE GOVERNANCE, RISK, AND COMPLIANCE

Providing trust for protected health  
information

## EXECUTIVE SUMMARY

Today's healthcare market applies different pressures to both payers and providers. Payers face intense competition that is driven by consumers who are demanding more flexible products, increased transparency, and better service. To survive and succeed, payers find themselves forced to adopt new business models. Health 2.0 is becoming reality, and with it comes expectations for participatory healthcare enabled by information, technology, and community.

Providers, on the other hand, serve an aging population with rising care expectations. These challenges exist against a backdrop of a shrinking supply of nurses and physicians. At the same time, consumers, payers, and employers demand efficient cost management and better outcomes.

For both payers and providers, healthcare remains highly regulated. The Health Insurance Portability and Accountability Act (HIPAA) already makes Protected Health Information (PHI) subject to strict privacy and security rules. Additional regulation is likely due to the Patient Protection and Affordable Care Act (PPACA), the EU Data Directives, and The Joint Commission. As competition escalates and organizations become more dispersed, and as regulations increase in number and complexity, risk inevitably grows. So, too, does the demand from markets, regulators, and customers for increased accountability.

The answer to managing and mitigating such risk is to bring governance, risk management, and compliance together in an integrated program where policies, data, and controls are strategically managed and visible throughout the healthcare enterprise. An enterprise governance, risk, and compliance (eGRC) strategy, supported by a common technology platform, creates consistency and transparency, enables collaboration, fosters operational efficiencies, and ensures the stability, continuity, and success of the business.

eGRC is not just another assemblage of solutions to address the same old problems. Rather, it is an innovative and multifaceted approach to a new paradigm, where healthcare risk management and compliance, as well as litigation issues, are seen not as isolated concerns but as closely related strategic initiatives with a direct impact on global healthcare industry objectives. These concerns, therefore, require the attention and influence of governance, which ultimately is responsible for the growth and performance of any business.

## THE EMERGENCE OF eGRC AS A BUSINESS IMPERATIVE

The emergence of eGRC as a strategy for protecting the healthcare enterprise and PHI from excessive risk, while removing barriers to growth, is the result of a number of factors including:

- Demands on corporate governance
- Increasing Electronic Health Record (EHR) adoption leading to greater risk
- Growing healthcare regulatory requirements
- Disappearing boundaries in the hyperextended healthcare enterprise

## DEMANDS ON CORPORATE GOVERNANCE

Governance refers not just to the people in charge of a business but also to the culture, policies, processes, laws, and institutions that define the structure by which healthcare companies are directed and managed. Governance affects how the company addresses everything from patient care strategies to day-to-day operations. Ultimately, though, when things go wrong, it's not the culture or the policies that are called to task, but the executives and the board of directors. An all-important area of accountability is the issue of whether internal and external constituencies trust that the healthcare company is doing everything it can to mitigate risk and protect the quality of patient care.

Current media coverage is also hot on the trail of healthcare companies that fail to protect sensitive patient information. Because of this media attention, the increasingly complex healthcare regulatory environment, and the devastating effects of a data breach, executives and board members are more closely attuned than ever as to how their healthcare businesses do business. This is certainly not a bad thing, but it means that those in governance need accurate, timely information about their company that is both broad and deep. Only then can they make decisions to stave off unnecessary risk, ensure compliance, and minimize the chances and impacts of patient litigation and regulatory penalties.

## INCREASING EHR ADOPTION LEADING TO GREATER RISK

Many healthcare organizations know what has to be done. They know that they must have a structure in place that clearly outlines data governance, business requirements, and the technology infrastructure and processes required to support a safe and secure PHI environment. However, these same organizations are also faced with challenges that include a lack of funding for security initiatives, increasing regulatory requirements and standards, and the growing need to share data with partners and collaborators. Add to this the fact that in many healthcare organizations, individuals and departments have undertaken their own IT initiatives—whether server-based applications or simple spreadsheets and databases—and it is easy to see how difficult the job of managing and protecting all of these data silos can be.

The increase in risk that arises from EHR adoption comes from a number of areas—from the dynamic and global nature of electronic information, to the growth in the amount of data that is going from paper to electronic media, to the use of electronic patient portals and collaborative patient care. With a more complex PHI risk environment, a more holistic approach to risk management must become a priority. A risk assessment of a healthcare organization's electronic environment is a good place to begin.

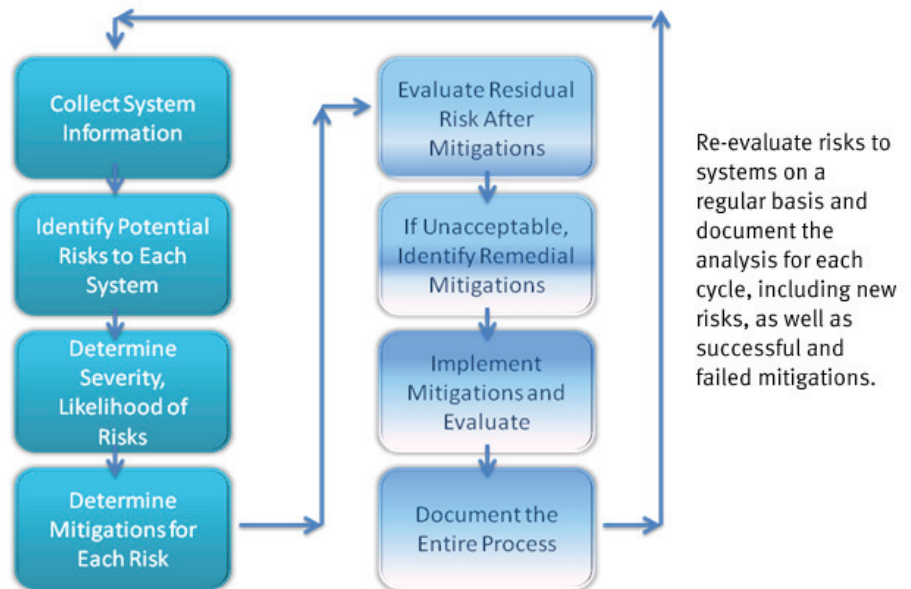


Figure 1. A Generic Risk Assessment Methodology

## GROWING REGULATORY REQUIREMENTS

Compliance refers not only to the act of adhering to regulations but also to a healthcare organization’s ability to demonstrate and sustain adherence to regulations—and not just externally imposed laws and regulations, but also internal corporate policies and procedures. Adding to the challenges are ever-increasing regulatory requirements, more serious penalties for non-compliance, more assertive (and global) regulators, and a more informed public.

Furthermore, managing compliance becomes increasingly difficult as much of the world moves toward principle-based regulation, which focuses on outcomes rather than checklists of requirements. Healthcare organizations are not told how to comply but rather what they have to achieve, which includes the ability to clearly document their compliance program and provide evidence of its effectiveness. There are multiple ways to achieve the desired outcome, and healthcare organizations need to chart their plan of action for reaching those goals. This requires integration of risk management practices with compliance—a new paradigm for many healthcare providers and payers.

## DISAPPEARING BOUNDARIES IN THE HYPEREXTENDED ENTERPRISE

Today, the healthcare industry is not a self-contained entity but instead represents an intricate, far-reaching web of relationships. Patient information is exchanged with more constituencies in more ways and more places than ever before. Technologies such as cloud computing, virtualization, social networking, mobile devices, and VoIP services—along with outsourcing—mean that the traditional boundaries of a single healthcare enterprise are disappearing. With all this cross-pollination of services and information, it can be difficult to define where one healthcare organization ends and another begins. This makes fertile soil for unwanted risk.

Managing hundreds or thousands of global entities that impact even a single patient’s information is a daunting task. In addition to the expected entities such as hospital labs, the ER, the OR, and Radiology, healthcare organizations are burdened with assessments related to

quality, facilities, environmental management, health and safety, security, privacy, workflow support, and employment practices. Still, organizations must validate that members of their extended enterprise (including business partners, contractors, consultants, outsourcers, and suppliers) are complying with laws, meeting their social responsibility practices, and operating in a way that does not introduce unnecessary risk.

New technologies create as many risks as they do opportunities. For example, a provider's use of mobile devices has a direct impact on that organization's delivery of their products and services, and creates new expectations for fast, seamless, and consistent experiences across various touch points. At each touch point, there is a chance to introduce risk, depending on how secure and successful the connection is and how well the organization is able to protect its patient's privacy when so much more personal health information is available for the taking.

## HEALTHCARE ENTERPRISE DOMAINS MOST AFFECTED BY eGRC

Four key domains within a healthcare organization are most directly involved in eGRC. They include IT, Finance, Operations, and Legal. In each of these domains, leaders must manage numerous policies around critical business processes and multiple regulations, and to each process, a control must be applied. Across the four domains, there is typically a significant amount of overlap and redundancy within the core processes of Policy, Risk, and Compliance Management. For example, different domains often deal with the same policies related to the same healthcare processes and regulations, and apply the same controls. Unfortunately, they are often not talking to each other, resulting in significant waste and inconsistency.

With an eGRC strategy in place, these domains would collaborate on their requirements, enabling them as appropriate, to apply the same control to different healthcare regulations. A hospital, for example, could use the same control to ensure compliance with both PCI and HIPAA. Authentication alone, as a control, applies to about 16 different regulations. It would be difficult and costly to manage these regulations manually, but eGRC enables a "one-to-many" process that reduces redundancy and repetition, improves efficiency and consistency, and keeps everyone aware of what's going on.

Consider the following risk and compliance issues faced within each domain:

**Information Technology**—The IT department has typically focused on technical EHR and infrastructure risk and compliance challenges, attempting to keep hackers, viruses, and worms at bay while maintaining systems in a state of recovery should a disaster strike. Today, with the onslaught of regulations, the IT department is struggling to build its own legal acumen to comply with increasingly complex laws and regulations, as well as manage policies that map to specific regulations, and tie those policies to controls. By taking a systematic approach, IT can eliminate its own silos.

**Finance**—In the early years of the U.S.'s Sarbanes-Oxley, Finance executives struggled to define internal controls, assess those controls, survive (let alone respond to) internal and external audits, defend financial performance results to stakeholders, maintain segregation of duties, and ensure the accuracy and integrity of financial reporting. Though demonstrating Sarbanes-Oxley compliance has become a much more streamlined process for many organizations, finance executives are still challenged to stay abreast of financial risk and internal controls over the full range of accounting processes.

**Operations**—Because Operations is where healthcare services are delivered, employees are managed, and customer relationships are maintained, this domain is on the front line of risks that could harm the provider/payer's business. From missed delivery schedules to

missed forecasts, supply chain breakdowns, internal policy violations, and patient touch point issues, there are innumerable potential trouble spots that COOs must monitor.

**Legal**—Legal is usually responsible for ensuring adherence to external laws and responding in the event of a violation or a litigation request. Legal knows only too well how compliance and litigation issues combined with both internal and external risks such as judgment, sanction, or fine can impact any business. Yet because risk is pervasive and regulations touch all business units, Legal can't be proactive and comprehensive in its work unless it has the ability to audit compliance efforts throughout the healthcare enterprise and identify which areas present the greatest internal or external risks of litigation against the company.

Because these four roles tend to work in silos and often lack a sustainable strategy for cooperation, they take varied approaches to ensure compliance and minimize risk. As a result of these redundant and inconsistent efforts, resources are easily drained, accountability and information-sharing (and therefore visibility) are lacking, and it is extremely challenging to correlate and prioritize the most pressing issues.

## THE RESULTS OF AN OUT-DATED APPROACH

Instead of treating each risk and compliance issue as an individual problem, healthcare organizations must look for a common approach to managing risk and compliance across the hyperextended healthcare enterprise. Organizations that don't achieve this level of collaboration are paying a significant cost in terms of wasted resources, increased complexity, decreased flexibility, and ironically, even greater exposure to risk that threatens a patient's quality of care.

We explore each cost briefly:

- **Wasted Resources**—Instead of prioritizing how resources can be leveraged to meet a range of needs, organizations tackle issues one-by-one, resulting in varying processes, systems, controls, and technologies. The excessive time and expense required to do this takes the focus away from business initiatives that can improve the bottom line.
- **Increased Complexity**—Inconsistent healthcare risk and compliance approaches introduce greater complexity to the healthcare environment, and with complexity comes increased inherent risk. When controls are not streamlined and managed consistently, there are more points of control failure and compliance gaps. Furthermore, inconsistency in controls means inconsistency in documentation of risk and compliance, which can further confuse the organization, regulators, and business partners.
- **Decreased Flexibility**—When a healthcare organization is spinning multiple risk and compliance plates, its ability to respond to other issues is compromised. The organization ends up doing a substandard job on the plate-spinning and sees its own performance suffer because it is less able to respond to emerging opportunities.
- **Greater Exposure**—With the focus on what is immediately at hand and not on what the provider/payer needs to protect itself from in the long run, an organization will find itself facing more present threats rather than fewer. Duplication of processes and gaps in coverage are bad enough, but when they aren't visible at the governance layer, the healthcare organization is at the brink of exposure to serious risk.

## THE PARADIGM SHIFT TO eGRC

Clearly, healthcare organizations can no longer afford to focus on risk and compliance issues separately. A new paradigm is needed—one in which multiple domains work together under a unified framework to ensure that processes and systems, as well as partners and employees, behave as a cohesive, well-governed unit.

Healthcare organizations must take a deep look into their long-term vision, and plan today for future risk and compliance challenges. While no organization can eliminate all of the complications of a rapidly advancing and transforming world, the better able it is to proactively identify and address pressing issues, the more likely it is to safely navigate through the waves of change and emerge successful on the other side.

At its core, an eGRC strategy aligns people, processes, and technologies across the IT, Finance, Operations, and Legal domains. Because no healthcare company has a Chief eGRC Officer, what's needed is a cross-domain steering committee that comprises the head of compliance, the general counsel, the CSO or risk officer, the head of audit, the controller's office, and the CIO. This committee would typically report to the finance head or the Chief Administrative Officer, and its success depends on how well stakeholders engage to share information and integrate their efforts for a holistic view of governance, risk, and compliance across the enterprise.

Senior executives must understand and acknowledge the interrelationships among governance, risk, and compliance—and be committed to having these processes work in harmony to increase collaboration, reduce uncertainty, and produce more predictable results. It is critical, therefore, to gain consensus on the goals of an eGRC program, which are as follows:

- **Accountability**—Healthcare organizations require a system of accountability where executives can see the status of issues, events, incidents, and unresolved findings, and hold individuals accountable for their resolution. Big-picture visibility of eGRC is necessary, along with the ability to drill down into specific areas.
- **Sustainability**—Healthcare organizations demand a sustainable process and infrastructure for ongoing governance, risk, and compliance processes that are becoming more plentiful and complex. As the healthcare arena changes rapidly, point-in-time assessments are no longer good enough by themselves. Healthcare is changing minute by minute, requiring that organizations address eGRC issues collaboratively and continuously.
- **Consistency**—Healthcare organizations need tools that force them to be consistent in their methodology and reporting so they can compare apples to apples. Without consistency, there is no way to effectively prioritize issues and resources. eGRC ensures that every critical domain and function in the healthcare organization knows the big picture and understands their role in it.
- **Efficiency**—Redundant assessments and audits looking for similar information for different purposes are wasting resources and hindering productivity. eGRC aims to ease this burden by leveraging common processes, assessments, and information across the enterprise.
- **Security**—Security oversight aims at understanding and modeling various threat likelihoods and impacts to select, as well as prioritizing controls to bring PHI systems and information in line with acceptable levels of risk tolerance.
- **Transparency**—Quality patient care demands transparency across key performance and risk indicators so it can monitor the organization's health, take advantage of opportunities, and avert or mitigate disaster.

## A PLATFORM APPROACH TO eGRC

Healthcare organizations may still rely on a document-centric, paper-based approach to risk and compliance management, rarely attaining sophistication beyond electronic documents and spreadsheets. Aside from being error-prone and inefficient, this approach makes it difficult to share information, thereby reinforcing silos. Embracing the EHR requires a technology architecture that integrates with other systems and provides for a cohesive and common

eGRC management platform. This platform should tie into healthcare enterprise applications and infrastructure, consolidating the information necessary to manage risk and compliance throughout the organization.

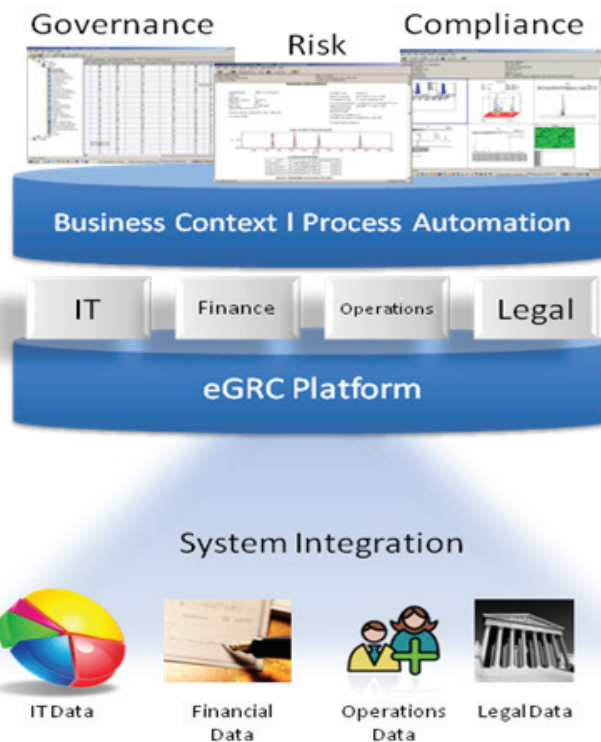


Figure 2. eGRC Platform Model

Requirements for such a platform include:

- **Centralized Views**—A central view of risk and compliance activities provides a single lens through which PHI stakeholders can identify threats early and prioritize issues, as well as improve efficiencies by applying a single process to multiple regulations.
- **Automation**—Through automation, healthcare organizations achieve continuous risk and controls monitoring as opposed to the point-in-time spot checks of the past. Technological capabilities required include advanced risk analytics and modeling, automated controls tied to business rules engines, advanced content and process management capabilities, and embedded eGRC control points.
- **Integrated Systems**—Multiple point solutions that span different areas of the infrastructure are costly to manage, fail to deliver a holistic view of the healthcare enterprise, and cannot correlate analysis to provide reliable conclusions. Integration facilitates management and reporting across the entire healthcare enterprise. (See “Information Integration and Healthcare Context” for more on this requirement.)
- **Flexibility**—An eGRC platform must be adaptable to evolve as the provider/payer evolves. Furthermore, users must be able to make changes and build out applications to solve problems without relying on costly, time-intensive custom development. Every healthcare business has different risk management and compliance requirements, so the eGRC platform must be tailored to an organization’s specific needs and structure.

## INFORMATION INTEGRATION AND HEALTHCARE CONTEXT

Healthcare organizations have an extraordinary range of data that is relevant to risk and compliance management as well as patient safety. However, in many cases this data is scattered across multiple tools and systems, making it extremely difficult to put risks, threats, incidents, and compliance deficiencies into a healthcare context, and prioritize the response

Examples of relevant risk and compliance data include, but are not limited to, the following:

(This list does not include the usual sources of patient data such as lab test results. Risk from these usual data sources would add more risk from additional areas.)

- Risk analytics (predictive modeling, simulation, and forecasting)
- Loss events
- eDiscovery
- Configuration scan results
- Security event logs
- Sensitive data discovery
- Document and records retention data
- Collaboration systems like Microsoft® SharePoint®
- Email
- Threat intelligence
- Vulnerability scan results
- Emergency notification call chains
- Asset and supply chain management data
- Customer and partner profiles
- Accounting and HR information
- Exceptional disaster recovery—VMware® vCenter™ Site Recovery Manager enables testing in isolation without affecting workflow

based on what is most significant to the organization. In order to pull in such diverse types of information from a multiplicity of sources, including proprietary solutions, an eGRC platform must be vendor-neutral and able to identify and correlate disparate data from all parts of the healthcare enterprise.

## HOW AN eGRC PLATFORM ENABLES RISK-BASED, HEALTHCARE-ALIGNED INTERNAL AUDITS

In an effort to provide more value to the healthcare organization, an audit's focus is shifting from compliance to risk, so instead of looking for control failures, the function is preventative, attempting to keep failures from occurring. Now that auditors are being challenged to validate structure, processes, policies, and controls across governance, risk, and compliance domains, an audit is becoming a key component in eGRC initiatives. This means that not only has the scope of work changed, but also the nature and the tools. While a learning curve is required, ultimately eGRC offers significant benefits for internal audits.

Currently: auditors have to piece together decentralized documentation captured in multiple healthcare systems. They lack visibility into existing risk assessments, and the audit plans themselves lack the flexibility to react to emerging risks and business concerns. There is also an inability to track the status of risk mitigation efforts resulting from audit findings. As a result, audits struggle to focus on issues most critical to the business.

With an eGRC Platform: auditors can coordinate information, priorities, and objectives among audit, risk, and compliance teams, and ensure that the audit plan is aligned with the healthcare organization's priorities and business objectives. External auditors can securely self-serve the information they need, and business units can manage and track their own findings and remediation efforts within the same repository as the audit department. With a consistent audit process and methodology supported through one centralized system, the organization benefits from higher-quality audit projects, more productive and efficient auditors, and a reduced risk of fines, loss events, and operational costs from unresolved findings.

## HOW AN eGRC PLATFORM ENABLES BETTER HEALTHCARE BUSINESS CONTINUITY PLANNING

Risk management in the realm of healthcare business continuity goes well beyond typical (and still quite serious) threats such as data breaches, potential litigation, diagnostic snafus, and patient and competitor issues. The very ability of the healthcare organization to operate is at stake, and the current tools in use to respond to healthcare business continuity issues are often insufficient. Furthermore, plans are not always updated, so they are based on old information formulated in a different context. Risk has to be classified based on impact and likelihood, and plans must be regularly updated.

Currently: as with audit, healthcare business continuity and disaster recovery teams are stymied by decentralized, static documentation captured in multiple tools and inflexible systems. They lack visibility not only into plan status, approvals, review dates, and testing, but also into emerging IT and business risks that can impact their plans. Because of this, there is uncertainty over which processes, technologies, and other infrastructure components need to be recovered first, and how to provide realtime response information to people who need to know where to go and what to do in a crisis.

With an eGRC Platform: healthcare organizations can better coordinate information, priorities, and processes among business continuity, disaster recovery, and crisis teams, ensuring that contingency planning is strategic (i.e., aligned with the healthcare organization's priorities and business objectives). Business-relevant reporting is generated automatically from

day-to-day plan maintenance, so plans are accurate, relevant, and accessible. Ultimately, an eGRC platform enables accelerated and appropriate response to crises, which reduces the impact of an event on patient care and revenue.

## DEVELOPING AN eGRC STRATEGY ROADMAP FOR HEALTHCARE

The web of healthcare stakeholders with varying requirements for governance, risk management, and compliance often results in a complex tug-of-war with opposing priorities. However, efficiency can be achieved through the definition of common processes and technologies that various parts of the healthcare organization can utilize for their individual requirements, as well as for collaboration and sharing. A successful eGRC strategy, therefore, is one that has a symbiotic influence on healthcare stakeholder roles and their common requirements.

Any healthcare organization looking to advance its risk and compliance efforts from tactical to strategic, and from isolated to collaborative, should begin by defining a strategic roadmap. An eGRC strategy roadmap is a multistage process that begins by identifying all of the healthcare business processes throughout the enterprise that fall under the eGRC purview. This is no small task as it requires determining the process owners and subject-matter experts, and getting those individuals together to create consensus over pain points, workflow, dependencies, complexity, the desired future state, and existing (and lacking) supporting technologies. Once this is completed, each healthcare business process must be analyzed to identify opportunities for automation and for eliminating redundancies (there will be many of both).

The results of these analyses are then delivered to a cross-functional steering committee (discussed earlier in “The Paradigm Shift to eGRC”), which is charged with defining the healthcare organization’s eGRC program: its vision, goals, components, stakeholders, and underlying technologies. Through this leadership team’s discussions, a tactical, phased approach to implementing the program emerges, along with a strategy for how it matures to its desired state. This plan must take into consideration both dependencies and redundancies to ensure an effective implementation.

It is important to note that eGRC isn’t just a technology buy. The success of an eGRC program depends on how well healthcare organizational stakeholders work together to share information and integrate their efforts to enable a holistic view of risk and compliance across the enterprise. Therefore, it is a combination of people, processes, and technologies that all must be aligned behind a common goal and commitment.

To sum up, the eGRC strategy roadmap includes these key phases:

- **Inventory**—Take an inventory of individual risk and compliance processes across the healthcare organization. This requires that the organization step outside of its internal silos and collaborate on a range of risk and compliance issues.
- **Analysis**—Identify which parts of the healthcare organization have strong processes and where processes can be improved, specifically by introducing automation and eliminating redundancy.
- **Goal-setting**—Outline where you want to be in three years and model the ideal eGRC strategy and implementation approach. Think outside the box so you are not locked into current approaches and processes.

- **Planning**—Build the plan to achieve the desired eGRC strategy and implementation approach. Identify the biggest eGRC challenges and address the most visible and inefficient issues first. Think big picture, but start in areas that can provide quick wins.

Of course, prioritization of risk and compliance activities must be decided at the PHI level to ensure maximum impact and sustainability. An eGRC strategy roadmap requires executive buy-in and support, which provides endorsement of the effort and overcomes the obstacles related to siloed entities wanting to work independently and do things in a proprietary way. As with any new paradigm, implementing eGRC requires a committed change management program.

#### THE EMC APPROACH TO eGRC

EMC Corporation ([www.emc.com](http://www.emc.com)), the world's leading developer and provider of information infrastructure technology and solutions, offers a rich portfolio of products and services for managing eGRC across all relevant domains. RSA®, The Security Division of EMC ([www.rsa.com](http://www.rsa.com)), delivers a foundational element to this portfolio—the RSA Archer eGRC Suite. This set of automated, integrated solutions, built on a common technology platform, enables a healthcare organization to centrally manage policies, controls, risks, assessments, and deficiencies across the enterprise, and report on its risk profile and compliance posture through realtime executive dashboards.

## CONCLUSION

One thing is certain: risk and compliance burdens are not going away. Government regulators continue to influence control upon healthcare organizational practices through tighter regulation, and patients are requiring stronger controls for security and privacy. The globalization of the healthcare business introduces significant risk with more points of vulnerability and exposure. The time is now for healthcare organizations to define and implement a sustainable eGRC strategy that drives accountability, sustainability, consistency, efficiency, security, and transparency. Selecting the right information infrastructure vendor, who provides for enterprise-level control and integration of risk and compliance, is a critical step that healthcare organizations should not take lightly.

Healthcare organizations face an array of technologies to consider for the foundation of their eGRC program, and the process for selecting the right vendor to build a sustainable eGRC program can be overwhelming. When evaluating IT vendors, healthcare organizations should consider the range of risk and compliance requirements impacting their business, and select a vendor that has the strongest integrated solution to manage these requirements on a consistent, ongoing basis. The right technology platform lays a strong foundation for a sustainable and effective eGRC strategy.

## CONTACT US

To learn more about how EMC products, services, and solutions can help solve your healthcare PHI and IT challenges, contact your local representative or authorized reseller, or visit us at [www.EMC.com/GRC](http://www.EMC.com/GRC).

EMC<sup>2</sup>, EMC, RSA, the EMC logo, and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware and VMware vCenter are registered trademarks or trademarks of VMware, Inc. in the U.S. and other jurisdictions. All other trademarks used herein are the property of their respective owners. © Copyright 2011 EMC Corporation. All rights reserved. Published in the USA. 3/11 EMC Perspective H8685