

Achieving Efficient Governance, Risk and Compliance (GRC) Through Process and Automation

A Low-Risk, High-Impact Approach
to Gaining Control of Regulatory
Compliance Before It Overwhelms
Your Organization

An Epicor White Paper

EPICOR®

Executive Summary

Now more than ever, organizations of all sizes and descriptions are struggling to comply with regulations and manage the risks and penalties of failing to operate within the rules. Establishing, maintaining and proving compliance requires both money and time that executives and shareholders would rather invest in top-line growth.

The myriad of procedures, tasks, and behaviors that bear upon compliance can be overwhelming. Yet organizations that can master the management all of these activities—and demonstrate that they have done it—operate more efficiently, compete more effectively, and build their brands and good names in the marketplace.

Fortunately, newly available software platforms that have become known as Governance, Risk, and Compliance (GRC) technologies can help. This paper discusses the drivers behind the growing awareness of GRC information technology and introduces the elements of an effective automated GRC system. It also presents a suggested method for a low-risk, high-impact approach to launching GRC automation.

Table of Contents

Introduction to Governance, Risk and Compliance	3
The Risk of Inadequate Compliance Management Systems	3
A Profusion of Point Solutions	4
Pinpointing Organizational Challenges	5
All Within Reach: Getting to GRC	6
Familiar Tools and Philosophies Fall Short	7
How Enterprise Applications Can Drive GRC	7
Enhanced Control with an Integrated Solution	8
Improved Financial Reporting	8
Financial Visibility – Budgeting, Planning and Forecasting	9
Supply Chain Visibility	9
Better Expense Management	9
Timely Visibility of Changes	10
Elements of an Effective GRC Software Solution	10
The Benefits of Effective GRC Automation	13
Conclusion	14
About Epicor	14
About Polivec	15

Introduction to Governance, Risk and Compliance

Taken individually, these three terms convey a range of meaning. But when grouped together, they have come to indicate a recently conceived category of technology and consulting services collectively referred to as *GRC*. An article in *CFO Magazine* suggests that the GRC category has its origin in software vendors that offer solutions to address Section 404 of the Sarbanes-Oxley Act. GRC was born when these companies recognized that they could alter their SOX applications, morphing them into more-complex and more broadly focused products that could address two related areas heavily affected by SOX: corporate governance and risk management.¹ The article goes on to say that GRC software "...at its core, remains a tracking system, capturing data on various compliance requirements as they affect a specific company and chronicling how the company does (or does not) satisfy those requirements." This straightforward description of GRC software serves as an effective basis for understanding its potential and its impact from a variety of perspectives.

It is important to realize, however, that GRC is not just about a streamlined, computerized index of rules. It is about behavior. A successful GRC platform is a powerful tool that enables a company to operate within the spirit and the letter of those rules. The behaviors and processes that the successfully implemented GRC platform catalogs and tracks become a part of the company's culture and of the work ethic of its employees.

The Risk of Inadequate Compliance Management Systems

GRC touches every person and every function in an organization in some way. Whether GRC becomes an intolerable burden that increases company overhead or an enabler of efficiency and success depends upon its actual, day-to-day impact on the employees' work and whether that impact is enabling or debilitating.

For most organizations, the latter is apparently still the case. In its 2007 GRC Strategy Survey, the Open Compliance and Ethics Group (OCEG) found that 65 percent claimed fragmented GRC caused serious business problems through duplication of efforts, redundant solutions, higher costs, and increased risk.² OCEG's findings are consistent with current research from industry analysts that cite fragmentation as a primary driver for GRC automation. Companies that have traditionally distributed compliance management responsibility across departments of the organization almost always experience duplication, conflicting systems, contradictory or inconsistent procedures and standards, and silos of information that

¹ "[One for Three](#): Should governance, risk management, and compliance be tackled as one problem, or is this a classic case of scope creep?," *CFO*, Sept, 2007

² [OCEG press release](#) "Survey Reveals Fragmented Governance, Risk, and Compliance Efforts Can Thwart Companies From Achieving Business Goals," Sept, 2007.

squander resources and increase risk from operating in a non-compliant manner.

This does not mean that GRC must be imposed from the top down. Rather, it must be *managed* from above and carried out by the individual departments, whose responsibility is to know and understand what they must do, and then do it. In other words, *accountability* for compliance remains “in the trenches” of the organization, but those who are there must know why they are required to do what they do in the name of compliance.

The Inhibiting Factors The true cost of compliance is difficult to estimate through modeling because there are so many variables and the rate of change among those variables tends to be high. As an example, one estimate put the cost to the U.S. economy for federal regulatory compliance in 2006 at \$1.14 billion. The number of regulations and the rate at which they change is often used as a measure of the magnitude of the regulatory compliance burden. In 1970, the Office of the Federal Register, referring to the Code of Federal Regulations (CFR), the official listing of all regulations in effect, contained almost 54,000 pages. That number pales in comparison with the 1998 data when the CFR totaled 135,000 pages in over 200 volumes. While some would disagree with how to calculate the cost of compliance, almost no one would argue that by any measure the cost is too high and that dramatically reducing the cost and complexity should be a top priority.³ Clearly, GRC is a fragmented endeavor in terms of both process and cost.

A Profusion of Point Solutions

To date, the few businesses that have attempted to employ technology to streamline compliance have taken a narrow, short-range “more is better” approach. The quick fix was to invest in one or more of hundreds of IT products across dozens of categories that are designed to address one or a few discrete aspects of compliance. Most of the investment has gone to products aimed at specific aspects of IT security. What has largely been overlooked is the critical need for tools to improve processes.

A recent study by Aberdeen Group reports that, “the preponderance of tactical, project-oriented point solutions often has the effect of end-user organizations acting as their own systems integrators – or absorbing the operational inefficiencies of managing a hodge-podge of discrete systems.” The report recommends instead a platform approach that, “starts with a consistent architecture to facilitate integration and interoperability for collection, archival, correlation, analysis, monitoring, auditing and reporting on security- and compliance-related data.”⁴

Until businesses expand their view of compliance from a narrow, event-driven project basis to a series of linked processes, they will struggle to get timely, usable information from their IT investments to drive sound business decisions.

³ The CFR is available on the worldwide web at <http://origin.www.gpoaccess.gov/cfr/>

⁴ Aberdeen Group, “[Sustaining Compliance](#), How I Learned to Stop Worrying and Love the Security Audit,” Sept 2007

Pinpointing Organizational Challenges

Because GRC affects every function in an organization, there are unique challenges associated with GRC that must be considered:

- **Unique business function requirements**
Each business function has unique needs that can often only be met with special systems, creating islands of information that do not support a macro view of trends and opportunities. This can also give rise to overly individualized processes and practices that don't extend beyond the borders of the given function or department. These practices, as well as the criteria for success and reporting mechanisms, are out of sync with the rest of the organization.
- **Entrenched legacy systems and processes**
Islands of information supported by stand-alone systems are difficult to integrate and usually too expensive to replace.
- **No agreement on who owns GRC**
Without a visible leader charged with GRC, multiple functions start separate initiatives or worse—nothing happens. Again, opinions differ on who that visible leader should be and there is no universal answer. The chief financial officer is a strong candidate to own GRC for a number of reasons. The CFO has an enterprise-wide perspective, is usually good at using technology and systems, has experience in implementing standards and guidelines, and knows how to determine ROI. However, one of the other members of the executive team may be a better choice, depending on how the company is structured and the nature of the business.

It can be difficult to decide who should be in charge, though. Consider, for example, the regulatory compliance measures that must be taken on matters relating to the issue of privacy. The breadth of senior level executive participation might require involvement of the chief executive, general counsel, chief compliance officer, chief privacy officer, chief information officer, chief technology officer, and the head of human resources. But while some participation of these individuals is to be expected in matters relating to issues such as privacy, it is highly probable that none of them would have the background, time, or inclination to assume responsibility for all aspects of compliance.

All Within Reach: Getting to GRC

While the GRC software and services category is fairly new, the need to act to take control of GRC is not. Businesses have been held to standards and regulations pre-dating Sarbanes-Oxley and similar standards. But these legislative changes help define and the concept of governance, risk and compliance.

Given its relatively short life, only a small percentage of businesses have begun investigating GRC solutions, and even fewer are very far along in the implementation stage. The risk of ignoring GRC is far greater than addressing it head-on. Without GRC you face the following hazards:

- Exposure to risk and liability of financial penalties stemming from compliance failure;
- Increasing fragmentation of people, process and technology;
- Excessive drag on the company that limits opportunities; and
- Wasted time and resources.

Besides minimizing these business traps, GRC comes with other benefits. Being known as a compliant organization burnishes your reputation and puts customers and potential customers at ease.

The primary question for those exploring GRC initiatives is not whether to do it, it's how to get started. Presentations and explanations by newly minted "experts" in GRC often have a discouraging effect on audiences painting a gloomy picture of the enormity of compliance and the complex nature of all the regulations and laws.

True, compliance is multifaceted and the laws can seem obscure and confusing. But in order to get started with a good compliance program powered by one of the new platform approaches, it is not necessary to boil the ocean. Rather, hone in on one particular topic or regulation that can be implemented without too much disruption to the business. Focus the scope of the implementation to ensure that tangible benefits are seen so the efforts can be validated.

This will set a foundation of competence with the GRC platform that can be adapted to deal with additional, more complex matters. With each successive regulatory problem that is addressed and overcome, the organizational learning curve shortens. Experiencing success in stages also engenders an appreciation for GRC and elevates the visibility of compliance to where it belongs in the hierarchy of importance within the company.

The GRC platform, properly implemented and enhanced through a series of successes, can be compared to a central nervous system for risk management and regulatory compliance. The platform should document and communicate policies and allow for easy, thorough auditing and management reporting.

Familiar Tools and Philosophies Fall Short

Companies expect their employees to work responsibly, performing their job in accordance with company policies and standards. But most employees don't understand the underlying reasons for the policies, nor are they equipped with the proper tools to help them perform their jobs within the rules. Similarly, they are often not trained to support compliance requirements, such as documentation and reporting. And those responsible for developing policies and procedures often don't appreciate the business impact. The high cost and effort required to update policies can cause them to become outdated, exposing companies to improper actions that lead to penalties and fines.

Bloor Research analyst Peter Williams describes the disconnect between policy implementers who are "down in the engine room who have to implement them within their means" and policy makers as two groups that don't speak the same language.⁵ Not surprisingly, policy implementers turn to common like spreadsheets to manage compliance which brings an array of risk factors.

According to the IT Compliance Institute, "organizations that rely on out-of-the-box Excel for their budgeting, planning, or business reporting requirements are taking unacceptable risks...it's almost impossible to configure out-of-the-box Excel to pass compliance muster when it's used in a distributed environment, with multiple, standalone copies of spreadsheets maintained on the hard drives of individual users."⁶

Spreadsheets should take a supporting role in GRC automation, relying on solutions that streamline and integrate GRC activities across business functions and across the company as the core resource.

How Enterprise Applications Can Drive GRC

Many companies will look to IT and software solutions to help them comply with GRC initiatives and improve their internal controls and reporting. Enterprise software applications can certainly help organizations document their internal controls, remove manual processes, and achieve greater visibility to their financial and operational data.

By implementing integrated solutions that ease the flow of information from the front office to the back office and by leveraging analytics and business intelligence applications, organizations are finding that software is a key component of compliance.

⁵ Peter Williams, Bloor Research, [IT Director](#), May 2007

⁶ Stephen Swoyer, [Conquering the Spreadsheet Compliance Nightmare](#), IT Compliance Institute

Enhanced Control with an Integrated Solution

Today, it is not uncommon for companies to use multiple enterprise software solutions in different divisions or even departments. Additionally, they may be running multiple instances or copies of the same software, and have a variety of stand-alone or point solution applications—such as for order entry or payroll—that are not integrated, or are integrated at a relatively low level. There may also be variety of separate databases, tools, and spreadsheets used for reporting, all which may be generating different versions of the truth.

Low-level integrations, which are often manual or manually controlled processes that consolidate the information, are particularly problematic as they can severely limit audit capabilities. Among other things often information needs re-entering from one system to another, opening the window for errors or tampering.

Even when the information moves automatically through an interface, there is often little or no opportunity to trace information from one system to another. This makes it more difficult for financial staff to investigate transactions, limiting the amount of auditing that can be performed within tight reporting schedules. It also makes it necessary for accounting staff to rely upon the assistance of gatekeepers who, in the event that they are concealing information, would be alerted by an inquiry and have the opportunity to cover their tracks.

Improved Financial Reporting

Organizations are under increased pressure to file accurate financial results faster than in the past. While spreadsheets may be providing an adequate solution today, as the deadlines shrink and controls become more stringent, they will no longer be a viable solution. Enterprise applications can help organizations meet these shortened deadlines in a variety of ways—from consolidating financial information to providing drill-down, drill-across access from financial reports to transactional detail. Ideally, organizations will strive to reduce the instances of their data or ERP solutions. If that is not possible, they must at least be able to consolidate financial results from their multiple instances. This consolidation should be automatic, fully auditable, and enable users to drill down from the aggregated information to the transactional detail.

As organizations improve their financial reporting capabilities to enable compliance, they should pay particular attention to making financial information more accessible. Enterprise reporting tools, portals, and other similar applications can be implemented to provide financial and operational personnel with the visibility they require to financial information.

Financial Visibility – Budgeting, Planning and Forecasting

Many companies also rely on basic tools to prepare financial budgets and forecasts such as spreadsheets and independent databases. In order to meet and exceed the spirit of the Sarbanes-Oxley legislation, which requires management to attest to the effectiveness of internal financial controls, companies need a more systematic process for financial budgeting, planning and forecasting. Sound corporate oversight over the budgeting planning and forecasting processes are also the most difficult controls to deploy across the extended organization given all of the various roles and responsibilities that need to touch a budget before it can be considered complete. Bottom line, when companies adequately plan, budget, forecast, and periodically review and update the budgets and forecasts, they exhibit a more mature level of internal control. A company that is unable to perform these functions well can play a major part in motivating financial fraud and not living up to the tenets of the SOX legislation. Integrated enterprise software applications go a long way in helping organizations document their internal controls, remove manual processes, and achieve greater visibility to their financial data.

Supply Chain Visibility

Reporting and visibility requirements affect more than just financial reporting. Full compliance places a heightened importance on supply chain visibility. Companies need to have visibility to understand and report on items such as purchasing commitments for materials, assets acquired by a supplier on a company's behalf, minimum volume guarantees to vendors, and contractual commitments to forecasts and orders.

To effectively report on these types of commitments and transactions, operations and finance will be required to work together more closely. Again, an integrated solution that incorporates supply chain functions with traditional enterprise applications capabilities will enable increased visibility to this information.

Better Expense Management

Expense management solutions such as strategic sourcing, procurement, and project management can all help a company improve internal control by improving visibility, communication, and control, while reducing risk. For example, procurement solutions help to automate the rules associated with purchasing goods and services and provide functionality such as workflow for approvals and spend analytics. Improving expense management and the controls around it can not only help an organization with GRC compliance, but can also result in significant savings.

Timely Visibility of Changes

Many of the requirements for GRC involve accelerated disclosure of information to external entities. This requires companies to have better visibility of changes than they had in the past. Business intelligence and enterprise performance management solutions will play a key role in keeping management abreast of changes in their business. These solutions enable organizations to quickly sift through data to find the trends that impact their business.

By using tools such as configurable alerts to monitor exceptions, managers can specify who needs to be notified when certain events occur. For example, an alert can be configured to tell a manager when certain regions are behind their forecast, when inventory has reached dangerously low levels, or when certain customers are beyond their credit limit. Business intelligence and other analytics solutions can go beyond telling organizations what is happening to helping them understand why it happened and even showing what might happen. Having solutions in place that can help you monitor your business will be critical as a company seeks to be in full compliance.

Elements of an Effective GRC Software Solution

In this section, we look at characteristics of software solutions that can effectively support GRC initiatives.

1. Fits With Your Business Priorities

An effective GRC solution must be general enough to address a diverse set of business needs, yet be capable of satisfying most or all of the requirements defined by a specific initiative. The ability for businesses to start with a single IT solution that improves one or more aspects of GRC today and at the same time establishes a sound foundation for more improvements down the road supports a low-risk, cost-effective, approach to better governance, risk and compliance management.

2. Supports Fast Time-to-Results

Today, when it comes to return on investments in IT technologies, executives expect measurable results quickly, especially with new technology categories such as GRC. In these cases, where prior knowledge and experience may not exist and therefore implementation carries a higher risk of delays, an effective GRC solution offers a quick path to measurable results. Ease of use and deployment are critical in order to minimize the operational time and effort to get up and running, but the built-in capability to track and document its worth in time and cost savings is just as important. Lastly, to support fast-time-to-results, the solution's ability to set the boundaries of an initial deployment to get demonstrable results in only weeks or months is critical.

3. You Can Extend Coverage Where You Need it, When You Need It

After you lay a solid foundation and prove value, an effective GRC solution supports extending the solution to additional aspects of GRC across the company. Further, it should support extending reach in accordance with your business priorities such as whether you want to pursue a new compliance initiative driven by an event such as an acquisition, or a new facet of GRC such as ensuring adequate policy coverage through more testing.

4. Easy to Try, Easy to Use

The justification for adopting GRC software is to simplify and streamline the systems and activities that enable effective GRC. Therefore the software must simplify, not complicate, the task at hand. The software must be easy to install, configure, and operate, and it should use commonly available technologies. Because GRC affects every business function, it should be compatible with current and future IT systems. To support the wide adoption of GRC across the enterprise, the solution should be approachable and usable by a wide variety of business users on a regular basis. In order to be easy to try, an effective GRC solution must also deliver significant demonstrable value within a department or business unit budget.

5. Leverages IT Systems

Much of the cost of employing hundreds or thousands of IT systems and applications lies in inefficiencies from duplication, incompatibilities between systems, and lack of sufficient resources to extract full value. The addition of new applications—from IT security systems to core integrated enterprise applications—propagates increasing volumes of disparate data, which makes it much more difficult to use information to drive business decisions. This is especially true in the realm of governance, risk and compliance where the need to connect people and processes with data is vital. An effective GRC solution connects with integrated enterprise systems to consolidate and utilize data from any source, thereby increasing the value of current IT investments.

6. How Data Auditing Fits In

Users with integrated enterprise applications have the ability to track and monitor most information that forms the basis of financial statements which are stored and maintained in databases, it is critical that these databases be subject to a continuous audit. A permanent audit trail of access and changes is the only way to validate what is actually happening and to monitor the preventive controls and processes intended to ensure data integrity. The combination of preventive controls with continuous monitoring gives executives and auditors the confidence to attest to financial results and associated IT controls. Data auditing supports compliance with other regulations such as FDA Title 21 CFR Part 11, HIPAA, Gramm-Leach Bliley, The California Senate Bill 1386, and Basel II.

7. Financial Visibility

These days any company still clinging to non-integrated spreadsheets and standalone general ledger-based reporting systems faces an uphill battle with instituting company-wide GRC initiatives. The benefits of integrated enterprise applications boil down to gaining not only more control and accuracy over financial visibility and reporting, but saving a substantial amount of time and money in the process as well for financial reporting.

8. Effective Segregation of Duties

A GRC focus on segregation of duties reduces risks by providing an internal control on performance through the separation of custody of assets from accounting personnel, separation of authorization of transactions from custody of related assets, and separation of operational responsibilities from record-keeping responsibilities. Consequently, access to functions, and even to information down to the field level, must be controlled in the application to accomplish this goal.

Before Sarbanes-Oxley, most companies underutilized the controls available within their financial systems. Sarbanes-Oxley forced companies to reevaluate the controls and configuration of their financial systems and spotlighted the concept of segregation of duties. Separating financial functions across individuals has always been good business practice to reduce the risk of fraud and check the accuracy of financial transactions. Integrated enterprise applications go a long way to enforce effective segregation of duties that meet mandates of Sarbanes-Oxley and other similar worldwide GRC legislative initiatives.

9. Configurable Business Process Management

Users with integrated enterprise applications can leverage the effective deployment of business process management processes while maintaining strict application security standards and upholding the integrity of segregation of duties. Organizational control and worker productivity are both enhanced with configurable business process management to facilitate inter and intra departmental security controls. A BPM system orchestrates activities, processes and ensures that all required rules are followed and all required steps are completed. As companies look to address new compliance issues like Sarbanes-Oxley or to achieve ISO9000 certifications, BPM becomes a critical corporate discipline.

The Benefits of Effective GRC Automation

Because of the extent to which GRC impacts the organization, it stands to reason that the benefits can be just as far-reaching. Three key benefits of effective GRC automation are:

- **Reduce the cost of managing compliance**
Enable employees and consultants to accomplish tasks in less time, eliminate redundant systems, and consolidate data through a unified approach to GRC.
- **Manage risk more effectively**
Reduce exposure to penalties that would result from failing to satisfy requirements by knowing as soon as non-compliance events occur, assessing their impact quickly, and taking appropriate action swiftly. Track relevant data along the way to demonstrate how the company does (or does not) satisfy those requirements.
- **Focus more on top-line growth**
When compliance activities are under control, efficiently being monitored and measured 24x7, executives and employees can invest more of their time on activities that drive revenue. Equally important, they can perform their jobs with more confidence and be more effective by knowing the risks and how to avoid them.

Conclusion

A rising tide of regulations is causing organizations of all sizes across every industry to take on more work in order to stay within the rules, prove that they are (or are not) and why. The burden of managing compliance cuts across the organization from board room to staff, employees to third parties, touching virtually every function. The problem has reached a boiling point where systems are breaking down, exposing organizations, their officers and shareholders to risk in the form of regulatory penalties and tarnished brands.

Treading water is not an option; organizations can and must master the management all compliance activities to operate more efficiently, compete more effectively, and build their brands and good names in the marketplace.

Newly available software platforms known as Governance, Risk, and Compliance (GRC) technologies can help. The right GRC technology solution can reduce the cost of managing compliance, manage risk more effectively, and reduce exposure to penalties that would result from failing to satisfy requirements by knowing as soon as non-compliance events occur, assess their impact quickly, and take appropriate action swiftly.

An integrated view of governance, risk and compliance is still a new phenomenon in the marketplace. Therefore, considering technologies that offer a low-risk approach that is capable of showing measurable results quickly makes good sense.

With the right technology solution, the entire organization can focus more on top-line growth, perform their jobs with more confidence, and be more effective by knowing the risks and how to avoid them.

About Epicor

Epicor Software (NASDAQ: EPIC) is a global leader delivering business software solutions to the manufacturing, distribution, retail, hospitality and services industries. With 20,000 customers in more than 140 countries, Epicor provides integrated enterprise resource planning (ERP), customer relationship management (CRM), supply chain management (SCM) and enterprise retail software solutions that enable companies to drive increased efficiency and improve profitability, and also empower global enterprises to achieve even greater success.

About Polivec

This whitepaper was written jointly with Polivec GRC which provides integrated, corporate-wide, software suite for Governance, Risk Management and Compliance (GRC) solutions across all industries. By providing an end-to-end business process for governance, Polivec enables corporations to manage risk, reduce cost, minimize complexity and protect their current investments. Headquartered in Mountainview, with offices in Washington and Colorado, Polivec is a privately held company, funded by Crimson Investment, an international, private equity firm located in Palo Alto.

Disclaimer

This document and its contents, including the viewpoints, dates and functional content expressed herein are believed to be accurate as of its date of publication, August 2008. However, Epicor Software Corporation makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims the implied warranties of fitness for a particular purpose and merchantability. Additionally, nothing contained herein is intended to or shall constitute legal advice. Epicor has used reasonable efforts in collecting, preparing and providing quality information and material, but does not warrant or guarantee the accuracy, completeness, adequacy or currency of the information contained in this presentation. All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. While the general descriptions of the regulations compiled, summarized, and presented are believed to be accurate and up-to-date at the time made, readers are reminded that laws and regulations constantly change. Accordingly, we cannot and do not make any representation, expressed or implied, that the information contained here is accurate and expressly disclaim that it can be used without independent legal or professional advice. Such information presented herein could be interpreted differently by any particular governmental agency or court. No one should act upon such information without appropriate professional advice after a thorough examination of the facts of the particular situation. All information contained herein is subject to change without notice. Epicor is a registered trademark of Epicor Software Corporation. All other trademarks acknowledged. This document and its contents are the property of Epicor Software Corporation. Recipients of this document should not distribute to any third parties without Epicor's prior written consent. Copyright © 2008 Epicor Software Corporation.

For more information, contact Epicor Software Corporation: info@epicor.com



Worldwide Headquarters
18200 Von Karman Avenue, Suite 1000
Irvine, California 92612
USA
Toll Free: +800.449.6772 (US/Canada)
Phone: +952.417.5207 (International)
www.epicor.com