KINETIC DATA

How to Streamline and Automate IT Compliance For the Enterprise

Implementing a proactive and risk-based information technology (IT) governance, risk management, and regulatory compliance (GRC) approach enables companies to better manage compliance costs and streamline compliance and business processes through increased automation.

GRC has always been an important if somewhat abstract concern to businesses, particularly companies that are publicly traded and/or in heavily regulated industries. Within the last decade, firms have developed a new and more concrete sense of urgency, as C-level leaders have been forced to address regulations such as Sarbanes-Oxley, Basel I, Basel II, and HIPAA, as well as mounting stakeholder and public demands for stronger internal controls and greater accountability.

High-profile corporate malfeasance, which wiped out billions of dollars in shareholder value early in the last decade, added to the growing awareness that governance, risk management, and regulatory compliance weren't merely nebulous concepts, but were instead important parts of a public company's DNA, as important as areas like product innovation, service delivery, and marketplace competitiveness.

Hence attending to GRC is rapidly becoming its own separate business discipline, although there is still some controversy as to exactly what it entails, why and where within the enterprise it's important, and how or if it should be integrated at the enterprise level.

What is GRC?

Michael Rasmussen at Corporate Integrity, LLC defines GRC in its broadest sense as follows:

- **Governance** is the culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed.
- **Risk Management** is the coordinated activities to direct and control an organization to realize opportunities while managing negative events.
- **Compliance** is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as corporate policies and procedures.[1]

While others may have their own definitions, nearly everyone who has studied the issue agrees on one idea: GRC is a process- and IT-driven effort. As such, its success or lack thereof depends on how well an IT group has its own GRC processes in order, and how effectively IT can help other functions within the enterprise manage their own GRC requirements and roll these up into an integrated enterprise-wide GRC view.

Indeed, while many would argue that GRC necessarily crosses numerous enterprise areas, including marketing, operations, and supplier and partner relationships, there is general agreement that financial GRC and IT GRC comprise the bulk of most enterprises' GRC activities.[2] These two activities bear responsibility for most of the legal and regulatory compliance requirements for data handling and protection. IT GRC efforts also directly affect how efficiently the department enacts its central role of supporting business processes and activities.

That's both good news and bad news for IT functions. It's good news because it increases IT's profile within the business and reinforces the notion that IT is the glue that holds the business together. It's bad news because most IT groups have enough on their plates already. No one can deny that IT departments are consistently under pressure to deliver a greater number of services faster and more efficiently, while facing continual budgetary pressures. These new services frequently require more approvals and more complex processes, and they often must meet greater regulatory

---

[1] http://www.corp-integrity.com/about/grc.html

[2] http://community.ca.com/blogs/iam/archive/2009/11/17/it-grc-towards-a-common-definition.aspx

requirements. This compounds the challenge of developing and adhering to effective IT GRC practices. Above all, the complexity of IT GRC activities can greatly increase the cost of IT at a time when most IT budgets are constrained.

What is IT GRC?

IT has its own specific GRC requirements, plus the additional mandate to support GRC activities across business units and at the enterprise level. A simple definition of IT GRC might be as follows:

- Using IT to manage the various processes of governance, risk management, and compliance of an organization;
- Ensuring that the implementation of governance, risk management, and compliance of all systems and IT process are properly conducted to support business operations; and
- Implementing a unified IT GRC approach, and managing the associated processes coherently to create operational efficiencies, provide visibility into IT processes, and ensure accountability.

But few things are ever simple in the IT world. IT departments often manage widely distributed networks and face multiple sets of regulations, as well as numerous internal and external audit requirements.[3] It's not uncommon for large organizations to be subject to audit requests from upwards of 20 internal and external entities and have 500–800 general IT control requirements. Partners and business customers, in turn, may require additional types of regulatory compliance or adherence to standards such as ITIL, COBIT or ISO 27001/27002 as conditions of doing business. Many enterprises must also ensure that suppliers and service providers are adhering to those standards.

[3] http://www.csoonline.com/article/674709/it-grc-tools-control-your-environment?page=1

Given the scope of the challenge and the relatively recent awareness of the importance of GRC, many enterprises do not yet have a robust, formalized, and automated method for tracking IT GRC controls. But that's exactly what's essential to meeting the challenge. As Paul Proctor, vice president of security and risk management at Gartner, and many others have argued,[4] "People are doing IT GRC, whether they are calling it that or not, but they are often document-centric solutions, using spreadsheets and other documents in some kind of shared repository."

Michael Rasmussen has noted, "Spreadsheets are a recipe for disaster. Eventually, they outgrow this; they don't have proper audit trails and it becomes unmanageable." [5]

The need for a "formalized and automated" approach to IT GRC is the most common refrain heard among analysts and corporate risk specialists. In the book, *IT Risks: Turning Business Threats Into Competitive Advantage*, authors George Westerman and Richard Hunter, characterize the approach as having "A well-structured foundation of IT assets—an installed technology base of infrastructure and application technologies, and supporting personnel and procedures—that is well understood, well managed, and no more complex than absolutely necessary."[6]

Daniel Magid, a noted IT compliance expert, has argued that there are six leading tools for cost-effective IT compliance ***(see sidebar)***, the most important of which, Magid says, is encapsulating compliance processes into an automated system, an effort that may require many companies to bring on new technology.[7]

There are a growing number of tools available today that address this main IT compliance challenge of encapsulating compliance processes into an automated system, but they are enormously expensive and most

Top Six Cost-Cutting Strategies for IT Compliance:

1. **Encapsulate compliance processes into an automated system.**
2. **Create structured, controlled software development processes.**
3. **Apply best-practice methodologies.**
4. **Collaborate, collaborate, collaborate.**
5. **Develop specific compliance reports/templates.**
6. **Bring on new technology.**

[4] CSOnline, ibid.

[5] CSOnline, ibid.

[6] http://searchcompliance.techtarget.com/feature/Chapter-excerpt-The-Three-Core-Disciplines-of-IT-Risk-Management

[7] http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=2501#author1840

fail the test of being “no more complex than absolutely necessary.” And while these tools are comprehensive, they often require IT organizations to undertake a lengthy process of mapping existing GRC processes or revamping those processes to meet the requirements of the new tools. And if these new tools don’t offer native integration with existing back-end IT management and security systems, creating an automated assessment and remediation of technical controls can involve extensive programming and customization, impacting IT budgets even more.

IT Compliance and Kinetic Request

So how does IT keep up with the demands of increased operational efficiency; adherence to governance, risk management, and compliance mandates; and cost reduction—all at the same time? By making the case to management for the need to buy an expensive new system and suffering all the implementation, testing, and administrative overhead that goes with it? Or by using technology to leverage the capabilities of existing systems?

For organizations that use established IT Service Management (ITSM) platforms, the second choice is often the most efficient and cost-effective one. ITSM platforms collect and manage data about IT assets and processes in a single, secure service management repository. By using additional technology on top of these platforms, this same data can be leveraged to automate compliance workflow activities at much lower cost than purpose-built compliance systems and with far less administrative overhead.

For example, consider the experience of a large international life insurance, pension and asset management company. The company’s existing IT compliance applications were largely homegrown and were buckling under the additional compliance pressures imposed by Sarbanes-Oxley, Basel I and II, and other new U.S. and European compliance mandates. The technology underpinning compliance activities was archaic and difficult to support. The company’s IT staff had more than 400 compliance tasks that needed to be conducted on a predetermined daily, weekly, monthly or yearly basis. As the number of compliance tasks continued to escalate, it became clear that the company could no longer rely on its existing compliance workflow processes, which were largely spreadsheet-based, increasingly time consuming and which exposed the company to unacceptable compliance risk.

Eventually, the company concluded that it needed an automated process to test appropriate processes and systems in order to provide evidence of robust computer controls for audit reviews, which were initiated by multiple divisions throughout the organization and by business partners. After a review of its options, the company decided to leverage third-party tools that integrated with its existing ITSM system and provided the degree of automated control it needed. This approach would allow the company to keep its compliance system in a stable and well-understood ITSM environment, rather than move it to a new purpose-built compliance environment, and would avoid the expense and long learning curve the latter option would have entailed.

In this company's case, the tool selected was Kinetic Request from Kinetic Data, which offered native integration with its ITSM system. Kinetic Request, a request management portal application, is bundled with Kinetic Task, a workflow automation engine. Combined, the applications allowed the company to add functionality to its back-end ITSM system that created automated workflows and approval processes for its existing compliance activities. In this way, the company avoided the expense of moving its compliance activities to a new environment. And by using Kinetic Request, the company easily automated the process of triggering preset compliance activities for its more than 400 different compliance tasks and the approval processes associated with those tasks. The benefits of this approach included:

- Moving compliance activities into a stable and known ITSM environment without the need to buy new hardware and IT management software;
- Reduced time and expense for completing compliance tasks;
- Visibility into dates and approvals critical for reporting to different auditors; and
- Reduced auditing and reporting costs.

KINETIC DATA

Summary

The use case described above is a practical example of how one company implemented a solution that almost perfectly matches Daniel Magid's top six cost-cutting strategies for IT compliance, the chief one being encapsulating compliance processes into an automated system. The key difference between the company's efforts and more elaborate automated compliance systems is that the company was easily able to map its existing compliance tasks to the workflow and approval processes built into Kinetic Request and leverage its existing ITSM platform to create a comprehensive and bullet-proof compliance system that perfectly suits its dynamic compliance environment. All of this was done without the expense and disruption of an entirely new compliance environment. In short, the company obtained the same functional results at a fraction of the cost.

A strong software compliance solution should *(more from Magid)*:

1. **Establish repeatable, automated compliance and change processes.**
2. **Link change-life cycle workflow to best-practice methodologies.**
3. **Include compliance-related report templates supporting standards.**
4. **Create centralized management and visibility of IT assets, as well as progress reporting for auditing and performance improvement.**
5. **Provide a collaborative communication infrastructure that ensures IT services and software initiatives support overall business goals.**
6. **Reduce IT costs by ensuring project teams build the application correctly the first time around.**
7. **Enable communication among stakeholders regarding all changes in projects, and ensure appropriate notification, reviews, and approvals.**
8. **Provide a secure, visible repository of all application artifacts.**

About Kinetic Data, Inc.

Kinetic Data offers the most extensive portfolio of third-party, software applications available. Kinetic Data has helped over 200 Fortune 500 and federal government customers—including General Mills, Avon, Intel, 3M, and the U.S. Department of Transportation—implement its award-winning BSM and service request management (SRM) applications aligned with ITIL best practices. The company has earned coveted recognition from the independent BMC Remedy user community—having received the "Best Customer Service and Support" award in 2010, and the "Innovator of the Year" award in 2009. Kinetic Data serves customers from its headquarters in St. Paul, Minn., offices in Sydney, Australia, and through a network of leading BMC Remedy reseller partners. For more information, visit *www.kineticdata.com*.