



Regulatory Compliance With Fewer Resources: A Framework for System i Shops

White Paper

Regulatory Compliance With Fewer Resources: A Framework for System i Shops

July 2007

Magic Software is a trademark of Magic Software Enterprises Ltd. All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.

Magic Software Enterprises has made every effort to ensure that the information contained in this document is accurate; however, there are no representations or warranties regarding this information, including warranties of merchantability or fitness for a particular purpose. Magic Software Enterprises assumes no responsibility for errors or omissions that may occur in this document. The information in this document is subject to change without prior notice and does not represent a commitment by Magic Software Enterprises or its representatives.

Contents

Introduction.....	4
Growing Pressure	6
Establishing the Framework for Achieving Compliance with Fewer Resources	7
Security First —but It's Not the Whole Picture	7
Augment the Solution with Third-Party Tools	9
The Increasing Importance of the Development Environment	11
Outsourcing the Rules.....	12
Conclusion	14
About Magic Software Enterprises	15

Introduction

If your System i shop is like most others, your development and maintenance staff is expending somewhere between 25 percent (on the low end!) and 100 percent of its development staff resources just to remain in compliance with regulations imposed on your company by forces from outside your company. In the U.S., these regulations and mandates might be coming from a multitude of sources: Sarbanes Oxley (SOX); local, state, and federal government tax and reporting requirements; accounting standards; industry standards like HIPAA for healthcare, PCI data encryption standards for the payment card industry, or Gramm-Leach-Bliley for financial institutions; environmental protection laws; and even mandates coming from the Department of Defense or Wal-Mart to implement RFID.

Internationally, document retention standards are being imposed on everyone. And European organizations are just as vulnerable to having resources consumed by compliance mandates as their U.S. counterparts as they face concerns from regulations such as Basel II. The Capital Requirements Directive (CRD) is the European Union's version of Basel II, the regulatory framework that will extend to all of the banking, financial and investment firms in the EU. One of the aims of the CRD is to remove existing national barriers so that EU financial institutions can more easily operate across the national borders of the member states. The regulations imposed by the CRD pose a major challenge to many of Europe's smaller financial institutions – and there are many of them.

Regulatory compliance threatens to consume significant resources that will draw away your attention from the projects that will increase your business advantage.

Regardless, then, of which side of the pond you call home, regulatory compliance is a real and present issue that threatens to consume significant

resources from your organization, drawing away your attention from the projects and initiatives that you have defined as those that will increase your individual business advantage

Until recently, many System i shops have perceived themselves as outside the target range of many of the most noteworthy regulatory compliance drivers. As smaller, privately held companies, they did not consider themselves as vulnerable to the flood of new and constantly changing regulations. But the day is truly past when companies of any size and type can avoid the issue. The Payment Card Industry (PCI) is making this evident. As Carol Woodbury, founder and CEO of [SkyView Partners](#), notes, payment card companies are now shifting liability to the banks and companies that issue the cards. Those companies are, in turn, shifting responsibility to the merchants. If you process and/or store credit card data, no matter how small or large you are, you are next in the liability chain. "TJX," says Woodbury, "is the poster child for security breeches since its failure to encrypt and store data properly, exposing more than 45 million credit and debit card numbers earlier this year." Bank of America and other multinationals may be able to withstand a financial hit of mammoth proportions and still survive—but can your company?

Achieving compliance with these standards and mandates—and remaining in compliance over time as those regulations are enhanced and expanded and updated—has become a major cost of doing business today. No longer do companies spend the majority of precious IT staff and system resources on activities designed by the organization to add value to the business. Instead, they find themselves treading water just trying to keep up with requirements imposed on them from outside sources.

Most System i shops find themselves treading water just trying to keep up with regulatory requirements imposed on them by outside sources.

Growing Pressure

The pressures on businesses of all sizes and types, then, are increasing at a fast clip, as new threats and vulnerabilities are identified and as companies also see the value of many facets of compliance as just plain old good business practices that, indeed, do bring value to the business on their own.

But System i shops (like many of their brethren on other platforms) have not been especially quick to embrace these mandates and regulations beyond what is necessary to pass the audit. As Clay Ryder, principal for [The Sageza Group](#), observes, "At this point, most System i users are simply bailing water just to remain in the race. They haven't brought in any new oars or anyone else to pull the oar. They are just keeping their heads above water—not moving forward."

Woodbury concurs. "The pressure of increasing regulations and compliance mandates is not likely to let up any time soon. On the security side, once companies bring themselves into compliance, they will presumably have to spend fewer resources maintaining that status. The big investment is in that initial phase. But from a trading partner point of view, technology is always going to be a moving target. Wal-Mart may dictate one thing one day and something completely different next year. In the development space, technology will always be changing, so the investment has the potential to remain high."

"In the development space, technology will always be changing, so the investment has the potential to remain high." – Carol Woodbury

Establishing the Framework for Achieving Compliance with Fewer Resources

There is a compelling need, then, for System i shops to establish a framework in which they can achieve and continue to maintain an "in compliance" status, employing best business practices but using as few resources as possible so that the business can stop treading water. The deployment of a development framework that can support and maximize flexibility, while reducing staff requirements, is clearly the answer.

To understand the way in which this can happen, let's look at the three primary solution components of a company's total compliance strategy, all three elements of which must be present if a full solution is to bring maximum value to the organization:

1. **Securing** the applications and the data;
2. Implementing **third-party tools** that can add compliance functionality to the system without requiring substantial staff resources; and
3. Orchestrating a development and maintenance approach that takes advantage of the benefits of **service-oriented architecture** (SOA) or platform-independent, reusable code to execute standard business processes across the entire enterprise, without the need to maintain those components individually for each platform, database, and application.

Security First —but It's Not the Whole Picture

For some time, many people in the System i world have equated, to a large degree, the achievement of a "secure" system with "compliance." After all, when the auditors came in with their magnifying glasses to look over the IT operation, passing the security audit was the primary goal. And it certainly

does stand to reason that if your computers and your data are not secure, nothing much else will matter.

The first component is security. But while security is a critical and mandatory component of compliance, "security" does not equal "compliance."

But while security is a critical and mandatory component of compliance, "security" does not equal "compliance," And those who stop at the implementation of system, data, and even network security alone may be ensuring that their companies will pass security audits—but they will not be addressing the full picture of the additional business benefits and best practices that can truly validate the company's widespread security initiative. The new regulatory environment, coupled with several years of particularly devastating natural disasters, finally got the strict attention of those in System i shops who, until then, often boasted that they really didn't need any external security because OS/400 was the most secure operating system around—which it was and still is. The high availability market picked up steam as did backup and disaster recovery services. The complacency of System i users was being shaken as some companies awakened to the fact that they were not even performing some of the most basic tasks. As Woodbury notes, "There are times when companies have difficulty doing some of the most rudimentary things like changing passwords on a regular basis.... In a lot of cases, a company simply hadn't realized that security and compliance have to be part of their business processes."

"Just because the System i is, indeed, the most securable platform in the marketplace," says Woodbury, "the functions that the operating system offers for security must be implemented properly in order to pass a compliance audit. In many System i shops, being 'securable' and 'being secure' are definitely not the same thing."

Furthermore, securing the box is a far cry from securing the network—the environment in which most servers operate today. The System i no longer sits on an island with the luxury of knowing that broader external (and even internal) threats will be threatening even the most basic of applications and databases.

The rush is on (or should be), then, to make the System i and its applications and data truly secure. Because of the highly increased pressure today from the Payment Card Industry, data encryption is front and center on the security agenda, and many tools and techniques are available to help companies make that often-difficult leap to true encryption.

Augment the Solution with Third-Party Tools

Fortunately, many third-party tools for security and for other aspects of the full compliance picture are available from a variety of respected vendors and these should be evaluated for their appropriateness in the company's portfolio of compliance tools.

According to Arjon Cohen, vice president of [Bsafe Information Systems](#), one reason that the need for such tools is increasing is the adoption of TCP/IP Networking for OS/400. Many business applications currently deployed on System i, including many ERP, banking, and financial packages, were designed before TCP/IP connectivity. While these packages restrict their users from accessing data natively through menus, their users have tools available on their PCs which allow them to access the System i database through the network.

Further, Cohen explains, while users can access the System i via their PCs, they typically bypass the menu security of the package, generating little or no audit trail. This can cause a big problem for any company aiming to achieve regulatory compliance. Basel II section 819, for example, requires banks to implement effective means for protecting proprietary and confidential information. Requirements like this have become a major driver for companies to buy packaged software to secure their System i in meeting regulatory compliance mandates.

Beyond the many third-party tools that are available to enhance the security requirements for compliance, many ISVs in the System i space additionally offer a plethora of other types of tools to help organizations face the difficult task of coming into compliance, remaining in compliance, and reporting results. These include tools that meet many of the challenging aspects of compliance, including vulnerability assessment, internal audit, user management auditing, document retention, archiving, reporting, and training—and more. Indeed, it's difficult to find a System i ISV that does not purport in some way to ease the compliance mandate challenge. And, while that might muddy the waters a bit in terms of determining which tools are right for your shop, it's heartening to know that so many System i ISVs have a full understanding of the compliance problem and have made such strong investments in providing solutions. This is just one more reason to applaud the value of the System i platform and to protect the investment that your company has made in it.

The second component is third-party tools. These include tools that meet many of the challenging aspects of compliance, including vulnerability assessment, internal audit, user management auditing, document retention, archiving, reporting, and training—and more.

Most of these stand-alone, third-party tools are worth looking at – especially those that address specific regulations in specific industries – and end users

are well advised to consider augmenting their security solutions with the appropriate set of third-party tools that are relevant for their environment. After all, these tools are tested and maintained by ISVs whose job it is to invest those coveted resources in having a tool available that's designed to do exactly what you want to achieve: save those precious resources for other core business development activities. The investment in these tools is well worth it and should be considered the second prong (after security) of the total compliance solution for your organization.

The Increasing Importance of the Development Environment

Those who are actively working to achieve any sort of regulatory compliance have quickly learned that the first challenge is simply understanding exactly what it is that the company needs to be in compliance with. This challenge is far from elementary. Experts in specific areas (taxation, health industry standards, SOX, PCI, etc.) are often the best people to provide help with that task.

A second major hurdle is identifying all of those applications that touch that process. It is conceivable that a business process, such as "calculate transfer tax," could be repeated hundreds of times in hundreds of applications. Never mind the initial implementation—the maintenance involved in keeping this function up to date as tax rules/laws change can be breathtaking.

It is in viewing these challenges that the benefits and importance of moving to a hardware/software/database-neutral, service-oriented development platform becomes clear. Adoption of such an approach to system implementation, componentizing the company's business processes for reuse across a wide variety of platforms both internal to and external to the company, resolves these issues.

When working with a metadata-driven, rule-based platform and development framework, many of the services that are common to compliance can be constructed one time and then deployed across all of the applications they touch, no matter what the platform or the operating system. It goes without saying that if a component can be built once and deployed multiple times, tremendous resources can be conserved. Rather than addressing compliance mandates application by application, they can be addressed from the standpoint of corporate processes that can be maintained and reused over and over again.

The third component is the development environment. When working with a metadata-driven, rule-based platform and development framework, many of the services that are common to compliance can be constructed one time and then deployed across all of the applications they touch, no matter what the platform or the operating system. If a component can be built once and deployed multiple times, tremendous resources can be conserved.

Defining components and business activities that are logically connected to one another is clearly more manageable to trace (an important aspect of compliance) than implementing the same processes multiple times in a huge array of end-to-end applications. Further, when new technology-driven compliance mandates such as RFID appear on the scene, less time will be necessary to build the application which can now be, at least in part, constructed from components of existing and proven applications, building on the investment that has already been made and greatly decreasing the time to deployment.

Outsourcing the Rules

A platform-neutral development environment allows companies to take better advantage, too, of a new trend in compliance: the outsourcing or "software as

a service" availability of detailed compliance processing and reporting in a very wide variety of industries.

Industries such as banking and finance, securities, healthcare, accounting, pharmaceuticals, and transportation are highly regulated. Simply keeping up with the changes to these regulations alone could potentially consume large numbers of resources. Today, many of these services required to do that can be purchased from the outside—and the number and quality of the services available are growing daily.

The outsourcing or "software as a service" availability of detailed compliance processing and reporting in a very wide variety of industries can save companies a great deal of development and maintenance effort.

As an example, Transaction Audit Group (TAG) headquartered in New York City, provides best execution reporting and analysis for the financial services industry. They maintain all of the feeds to the stock exchanges and each day apply the industry regulations for stock trades—along with their clients' individual, internal rules—to determine if the execution of the transaction has complied with the appropriate rules for that trade. They then issue compliance reports that are used by the client to satisfy SEC reporting requirements.

Similar services are popping up across many industries, and for many applications such as human resources reporting (e.g., sexual harassment, COBRA, EEO), and accounting, delivering the necessary internal and external report, and negating the need for the customer to maintain the detailed databases or establish the feeds directly into their own systems.

Having a single neutral development and deployment platform in place makes use of these services much easier to manage. Each application will "call" the

exact same process in exactly the same way. The service provided by the compliance vendor does not have to be concerned with linking to a particular database or the programming language used for the program.

Conclusion

Compliance is a huge and potentially complex task that is a fact of doing business today. We cannot avoid it. Neither can we become complacent that implementing tight security measures and passing an audit has solved the problem. The good marks that the System i gets for having a highly securable box will still provide seamless integration to secure the network, take care of intrusion detection, or choose or deploy the right data encryption tools for your situation.

Much of the System i community is just beginning to review its strategies for leveraging its investment in the System i across the enterprise and the business chain. The time is right for these two issues—the identification of a more flexible and modern development environment, and compliance—to be evaluated together and viewed in synergy with one another.

How will System i shops respond to this challenge? Sageza Group's Clay Ryder predicts that the path may be bumpy at first. "There are sound reasons why they should be looking hard at their development environments and the ways in which those environments do (or do not) impact the compliance picture. At first, there will be resistance. If they are going to continue to operate in the castle with the moat around it, as they have in the past, it's going to be very difficult for them to take advantage of the benefits and they will not be able to play in a much more loosely coupled, dynamic environment like service-oriented architecture if they cling to the past architectural point of view."

For all of the reasons that service-oriented architecture can bring value to an organization—reusability, flexibility, and ability, along with immense increases in productivity—it is an entirely appropriate justification for facing the compliance challenge. By building and managing the business processes themselves at a level above and away from any single database or operating system or hardware platform, you stand to save money many times over by not having to rewrite that process again and again for each different environment.

If a portion of the resources that you are spending today on compliance can be decreased, those hours can flow directly back into the business so that your staff can spend that time doing activities that the company itself has determined are best for the business.

The goal, after all, is to have a secure system, to satisfy the auditors, to implement the best business practices for your company, and, finally, to do it all in a way that can free up the maximum amount of resources so that your company can focus on those initiatives that will drive the bottom line. If that 25 percent or 50 percent or 90 percent of your resources that you are spending today on compliance can be decreased, those hours can flow directly back into the business and your staff to spend that time doing activities that the company itself has determined are best for the business.

About Magic Software Enterprises

Magic Software Enterprises (NASDAQ: MGIC) has been a leader in enterprise application development, deployment and integration technology for more than two decades. The company's service-oriented platform is used by companies worldwide to develop, maintain, and deploy both legacy and new business solutions, while integrating these applications across both internal and external, heterogeneous environments. Magic Software's platform-



independent methodology lets companies achieve agility by quickly assembling composite applications, allowing programmers to create services and architects and business analysts to orchestrate and reuse these services to enable business processes. Through partnerships with industry leaders such as IBM and SAP and more than 2500 ISVs worldwide, Magic Software technology is used by more than 1.5 million customers around the globe.

For more information on Magic Software Enterprises and its products and services, visit www.magicsoftware.com.