Compliance Deconstructed

JC CANNON AND MARILEE BYERS, MICROSOFT

The topic of compliance becomes increasingly complex each year. Dozens of regulatory requirements can affect a company's business processes. Moreover, these requirements are often vague and confusing. When those in charge of compliance are asked if their business processes are in compliance, it is understandably difficult for them to respond succinctly and with confidence. This article looks at how companies can deconstruct compliance, dealing with it in a systematic fashion and applying technology to automate compliance-related business processes. It also looks spe-

cifically at how Microsoft approaches compliance to SOX (Sarbanes-Oxley Act of 2002).

COMPLIANCE DRIVERS

Regulatory legislation and corporate governance are primarily what drives compliance. Failure to comply with legislation such as Sarbanes-Oxley can lead to fines and disruption of day-to-day business. Even companies that are not concerned with regulatory legislation need to protect important corporate resources such as customer data and trade secrets.

**When you
break it down,
compliance is
largely about
ensuring
that business
processes are
executed as
expected.**

These compliance drivers are leading to increased concerns about how policies might affect business processes, ranging from who can approve salary changes to which paper supplier to use. For most companies the main driver for compliance should be those processes that affect the bottom line. This is a good reason for conducting a formal compliance assessment as the first step toward beginning a compliance program. A compliance assessment can identify poor or missing processes that could negatively affect the company's value.

Compliance is not a new phenomenon and is not unique to enterprises. Teachers want their students to comply with class requirements. Police want citizens to comply with laws. Parents want their children to comply with certain behaviors. Validating that their children are adopting a desired behavior, however, is difficult. For example, parents can tell their kids to stay away from adult Web sites and be careful about sharing information with strangers on the Internet, but it is difficult to know that their pleas are being heard. If it is hard to ensure compliance in your own household where there

Compliance Deconstructed

is a high level of control, trying to ensure compliance at a company with 1,000 employees is a daunting task indeed. The lesson here is that *validation* is the essence of compliance.

Compliance is simply about ensuring that business processes are executed as expected. Many companies are concerned about the onslaught of legislation and the possible fines for non-conformance with mandates. They often rush to add tighter physical security, refining access permissions on file shares and internal Web sites and investing heavily in encryption technology, without looking at how those activities are tied to business processes.

Does adding an encryption feature to a product help enterprises address their compliance needs? Not unless it can be managed centrally by an IT administrator and its effectiveness in protecting data can be validated in a report. Otherwise, how useful can it be? Technology investments are fine, but they should be capable of enforcing the IT controls and business processes that have been defined for a company. In addition, there must be a way to validate their effectiveness. Although encryption is an important technique for protecting sensitive data, if a company has to deploy it manually on thousands of computers with no way of proving it is effective, it will not be of long-term value to the company.

Let's consider another household example. Most families have locks on their doors, but if they go on vacation for two weeks, can they say with certainty that no one has entered their home? Even if the house has an alarm system, it's hard to be certain that the house has not been entered. What if the same house had each room continually scanned with a camera that forwarded the images to the homeowner's phone? The homeowner could be warned if someone was moving inside the home or if the monitoring system was deactivated. This would provide better proof than a lock or an alarm system.

Now let's map that same issue to an enterprise where a CIO may be responsible for the protection of thousands of resources. The deployment of permission settings and encryption cannot validate compliance. For example, if a CIO wants to prevent insider trading, he or she could

place strict access permissions on all acquisition content and even encrypt the most sensitive data. If an auditor asks the CIO, however, to verify that only people who are part of the acquisition team have viewed acquisition documents, the auditor doesn't want to see an encryption setting. The CIO should be able to produce reports validating that only members of the acquisition team had access to the acquisition documents during the acquisition period. This can be done only through access logs that can be easily fed into reports that answer questions such as:

- Who accessed protected content during the acquisition period?
- Did each person have a need to access the content?
- Did the membership of any security group for the content ever change?
- Was all acquisition content protected during storage and transmission?
- Was any acquisition content ever transmitted outside of the scrutiny of the company?

These questions all address the essence of compliance—validation.

Consider the real-life example of an enterprise policy management software company that wanted to help companies place sophisticated controls on who could access sensitive data. Before the system could be deployed, all sensitive data had to be assigned to a set of categories such as medical or financial, and each employee had to be assigned to a role. Then rules could be applied to the data to control access. For example, data of a specified *category* could be accessed by individuals in the appropriate *role* for approved *purposes* under certain *conditions* with a few allowed *exceptions*. This appears to be the type of system that most companies would want to help them address compliance, but the software company found time and again that most companies were concerned that such a complex system could bring normal business processes to a halt because of poorly written policy. They were more interested in a system that would simply tell them where their data is and who is accessing it, especially those accessing it inappropriately.

TACKLING COMPLIANCE THROUGH CONSOLIDATION

Many companies have separate teams focusing on specific types of compliance. This can cause duplication of effort and result in conflicting policies. Although more than one piece of legislation can call for the protection of personal information, a company shouldn't have multiple policies that instruct employees on how to protect the same type of data.

Consolidating the management of compliance can lead to the creation of a single corporate compliance policy. In this manner, addressing new compliance legislation is a simpler matter of temporarily assigning a couple of people to deconstruct the needs of the new legislation and updating the single policy where necessary.

Some companies attempt to create policy at the corporate level and apply it to each department. This can be impractical for companies with diverse departments. Ensuring that the policy is meaningful to each department and is updated as processes evolve would be unmanageable.

A better approach is to create corporate policy that provides a high-level view on how business processes should be managed. Each department should then adapt

the policy to its own business processes. For example, the corporate policy can define sensitivity levels to be applied to all corporate data and can mandate that all data at the highest sensitivity level be encrypted. Each department can determine which data that it handles falls into that category and can ensure that it is encrypted. The departmental policy should, of course, be reviewed to ensure that it does not conflict with corporate policy.

AUTOMATING COMPLIANCE

After a company has performed a compliance assessment and put in place a set of controls to manage risks identified by the assessment, it should determine how to automate the controls. Automation should not be attempted before validating that the controls are appropriate for addressing the company's compliance needs.

Why automate? Implementing business processes using paper, e-mails, or disjointed files and applications is prone to error. There are too many opportunities for something to get lost or overlooked. In addition, audits can be expensive, laborious tasks when done manually.

When a company is ready to automate, it should look for a system that provides end-to-end control over busi-

A Case Study in Software Configuration Management

Configuration management is a compliance area that can have an enormous impact on a company. Here we examine just SCM (software configuration management). IT configuration management, however, can include operating system, application, network, and hardware settings. The software that is installed on a computer system can affect CPU and network performance, licensing costs, virus proliferation, and the efficiency of employees. For this reason, IT professionals want to be able to ensure that each computer in their scope is running the right software.

SCM starts with an assessment. You should obtain the assistance of experienced professionals from companies such as Accenture and PricewaterhouseCoopers to assist you. The assessment should look at the various computer roles needed to manage each company task. Possible server roles include: Web, authentication, database, development, file and printer, and accounting.

For each server role, you need to determine the appropriate operating system and application software. You may also need antivirus software and other programs that are needed for every computer. You need to track the version of the software, as well as number of copies licensed. A risk

management assessment will determine the importance of each role, which will then be used to manage the roll-out of changes. At Microsoft, SMS (System Management Server), along with other tools, is used to ensure compliance with configuration policies.

Once all computer systems have been properly configured, you need to create a plan for managing updates for security fixes, service packs, and new versions of applications. You should include a plan for validating changes in a test lab before deploying the changes to production machines. High-priority machines, as defined by the risk management assessment, should be updated first, followed by medium- and low-risk machines. You should include a contingency plan for when things go wrong and oversight to ensure that only the appropriate changes are occurring.

Once the SCM plan has been completed, there must be a way to track changes and validate to auditors that risks associated with software changes are being managed in accordance with corporate policy and, more importantly, regulatory requirements. SMS performs that service for Microsoft.

ness processes. The system should have strong reporting capabilities. For example, a company may want the provisioning for a new employee to be connected to a workflow to ensure that the employee is added to the appropriate systems with oversight. Any compliance system should be able to answer these questions: Why did an action occur? Who approved it? Automated security and workflows aren't going to help much if there is no automated way of determining if they are working.

Once an assessment has determined the business processes that need to be automated, it will be necessary to find systems that assist with the automation process. Microsoft's Regulatory Compliance Planning Guide (<http://www.microsoft.com/technet/security/topics/complianceandpolicies/compliance/rcguide/default.mspx?mfr=true>) describes 19 technology solution areas that provide guidance and information on technology for automating the compliance process.

SOX COMPLIANCE AT MICROSOFT

Compliance with the Sarbanes-Oxley Act at Microsoft is an integrated program that includes the following components:

- Annual SOX 404 management assessment
- Quarterly SOX 302 compliance
- Disclosure committee oversight
- Internal audit and external audit oversight

ANNUAL SOX 404 MANAGEMENT ASSESSMENT

Scoping. Microsoft's annual assessment of internal controls to comply with Sarbanes-Oxley Section 404 requirements begins with evaluating scope. The company deconstructs its financial statement line items into cycles and subcycles. For example, a *cycle* within Revenue would be MSN Advertising and Subscriptions revenue, and Subscriptions would be a *subcycle*. Each subcycle is then dissected to find the locations that contribute the significant dollars—Redmond, for example. Subcycle locations are determined to be in or out of scope based upon quantitative and qualitative risk factors. Typically the in-scope subcycle locations include more than 90 percent of the

company's financial statement transactions and balances. When a subcycle/location combination is determined to be in scope, Microsoft identifies the transactions or processes that generate the financial statement information. Figure 1 illustrates the scoping process.

Control identification. For each transaction identified for in-scope subcycle/location combinations, Microsoft determines the risks of incorrect or missing accounting information, sets control objectives in response to the risks, and then finds the key controls that ensure that the risks are adequately mitigated. Key controls are both manual and automated application controls. Transaction flows and key controls are documented in narratives and flowcharts.

As an example, for advertising revenue, a risk would be that revenue is not properly recorded in the general ledger. The control objective would be that revenue is properly recorded in accordance with local accounting practice, which follows GAAP (generally accepted accounting principles). A key control is a reconciliation of revenue recorded in the order system, the sales system, and the general ledger.

Typically, key controls identified for SOX have been activities that are already taking place in the accounting process. The challenge is not in finding adequate key control activities but in narrowing down what is considered important.

Key lessons learned in the processes of scoping and control identification include:

- Choose the correct focus. For each in-scope transaction, identify the relevant financial statement assertions, such as valuation, completeness, or segregation of duties. Eliminate any irrelevant assertions.
- Concentrate on probable risks to the accuracy of the financial statements. Recognize operational-only risks and remove them from consideration—for example, inefficiencies in a process usually do not pose a financial statement risk.
- Find the right balance between a centralized and decentralized approach. For some types of transactions, such as financial closing processes, imposing standard

controls across locations is a good idea. For other types of transactions, a decentralized approach with each location finding its own key controls makes more sense.

- Focus on higher-level analytic controls rather than detailed process controls. Most companies learned this lesson in the first two to three years of SOX compliance and have eliminated a large percentage of the key controls that were originally identified. In many cases, the financial statement risks are adequately mitigated by higher-level controls performed later in a process. The more detailed process controls are still important but do not need to be tested as key SOX controls.

IT Controls. After the scope of business processes is determined, each process is linked to the application(s) that support the information capture and reporting. Applications that are found to be in scope are then associated with the IT group that supports each application. Infrastructure elements associated with in-scope applications, including databases, operating systems, and hardware, are also brought into scope.

Microsoft uses standard control objectives for applications and supporting infrastructure elements that cover the following key objective areas: access controls, interfaces, databases, software development lifecycle, maintenance, perimeter network, operating system patch management, backup, physical security, and operations.

As with business processes, Microsoft finds and documents key controls that satisfy the control objectives for each application and IT group. These types of controls lend themselves to standardization, testing the same or similar controls for each application and IT group. Consider again the example of advertising revenue: The company must properly restrict access to particular functions within the systems that process revenue, and it should test controls over the systems' ability to restrict access, as well as the process of granting and reviewing access.

Assessment. Once all key controls have been specified and documented, the company evaluates the design of the controls and then develops testing plans to perform the management assessment of operational effectiveness. Controls are tested each year, typically before the end of the seventh month of the fiscal year, and then are reevaluated before the end of the year through update testing. The testing of controls is performed by peer testers, external contracted resources, or internal audit in the course of a normal audit schedule.

The reconciliation control described previously might be tested by choosing a sample of one or more reconciliations (depending on frequency) and obtaining and reviewing evidence that the reconciliation was properly performed and reviewed and that reconciliation items were investigated in a timely manner. The test evidence

would be documented and retained as part of the SOX compliance work papers.

Evaluation of Deficiencies. If deficiencies are discovered in either the design or operational effectiveness of controls, management and internal audit evaluate them for significance and pass them on to the external auditors. Microsoft evaluates deficiencies as part of the quarterly reporting process.

QUARTERLY SOX 302 COMPLIANCE

To support the quarterly 302 certifications of the CEO and CFO, Microsoft has established a quarterly process of surveys and sub-certifications. Throughout

Compliance Deconstructed

the organization, controllers, subcycle and subcycle-location owners, and finance executives complete a variety of surveys to assess the effectiveness of disclosure controls and procedures, internal control over financial reporting, and changes in controls. This process involves approximately 250 individuals. The responses to all surveys and requests for information are analyzed and incorporated in the quarterly deficiency analysis as appropriate. Changes in the control structure are also evaluated for significance and possible disclosure.

DISCLOSURE COMMITTEE OVERSIGHT

The results of the SOX compliance program are reported quarterly to the disclosure committee, which includes key finance leaders throughout the company. The committee reviews the results of the quarterly evaluations of deficiencies and changes in controls and reviews updated risk assessments.

INTERNAL AUDIT AND EXTERNAL AUDIT OVERSIGHT

Microsoft's SOX compliance program is subject to audit by both internal and external auditors. Management works closely with both of these groups to coordinate planning, testing, and evaluation of test results.

PEOPLE AND ORGANIZATION

Because Microsoft is a large, global organization, its SOX compliance program is decentralized. The corporate financial compliance group administers the SOX program, sets policy,

determines the plan for the year, provides training, and coordinates the evaluation of deficiencies. Each business group, region, and operations center has one or more controls and compliance managers who provide first-tier support to the field. Each subcycle and subcycle location has an owner with primary responsibility for documentation and assessment of processes and controls.

The SOX program organization is illustrated in figure 2, along with approximate numbers of people involved in fiscal year 2006.

As might be expected, managing a global, decentralized compliance program is challenging. Key success factors in the Microsoft program are:

Strong senior management sponsorship and guidance from the beginning. The CEO and CFO placed high importance on successfully implementing the compliance program, and this commitment was well known throughout the company. This sponsorship and high level of

commitment exists at all levels of company management.

Good program design, with accountability pushed out to all locations from the outset. Unlike many other companies, which had to roll out a corporate program to the field in the second or third year, the subcycle and subcycle-location owners have always had primary responsibility for compliance.

Consistent guidance and communication from the central team. Although communication can always be improved, Microsoft technologies enable realtime status tracking and reporting via input into the central SOX compliance database and regular outward communication of guidance and updates via biweekly LiveMeeting sessions that are accessible globally.

TECHNOLOGIES

Since Microsoft was initially in the earliest SOX compliance deadline group, it had to be selective in the elements it chose to incorporate in a system solution. The company knew that its abilities to version documents, maintain audit trails, and provide secure access were critical, and it used Microsoft SharePoint software to meet those requirements.

With the change in filing dates, Microsoft's SQL Server team took the opportunity to try to make the organization of controls and reporting processes more efficient. Because the organization of controls and test data requires a unique hierarchy for easy administration (starting at the financial statement class and expanding down to the individual control objectives and activities), the team built an application that would allow users to navigate easily to their areas of responsibility and document and record their controls and test results. Using SQL 2005 as its implementation platform, the team also integrated flexible online reporting to monitor status and provide updates for field, management, and executive reviews.

CURRENT STATUS AND FUTURE OBJECTIVES

Since Microsoft's fiscal year ends June 30, the company has just completed its second year of SOX compliance. (There was a "Year 0" in FY04 since the deadline was extended after the company had completed much of the initial compliance work.) Over these three years, Microsoft has successfully reduced its scope and key control testing by more than 50 percent as a result of improvements in risk assessment and controls rationalization. The company has worked to standardize controls and focus on higher-level analytic controls where possible to eliminate detailed and/or redundant process-level controls.

A key success factor has been the decentralized

approach, which assigns ownership and accountability to people with appropriate authority throughout the organization. Its enabling technologies allow Microsoft to manage a decentralized program effectively. Objectives for the future include continued improvement in the effectiveness and efficiency of the program, while maintaining strong internal control structure and timely remediation of deficiencies.

STEPS TO SUCCESS

Individuals entrusted with compliance should not permit the pressure of regulatory requirements to force them to make hasty decisions about addressing compliance needs. Instead, follow these steps:

- Work with an internal or external compliance expert to perform a compliance assessment.
- Create a set of IT controls to address any high-risk business processes.
- Consolidate compliance efforts into a single corporate compliance strategy.
- Have each department define a strategy to comply with corporate policy.
- Use technology to automate the creation, enforcement, and deployment of policy.

The work of compliance will go more smoothly once you have created a set of IT controls to address risks that were found during the assessment process. Using technology can help to streamline and automate the definition, enforcement, and validation of IT controls. Most importantly, before starting any compliance program, get assistance from a reputable auditing firm. □

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

JC CANNON is a senior program manager in charge of compliance strategy for the SQL Server team at Microsoft. He is tasked with helping to ensure that SQL Server's new data platform contains features that help companies fulfill their privacy and compliance needs. He will also focus on ensuring that SQL is a robust platform for developing effective compliance solutions.

MARILEE BYERS is the group manager for the Financial Compliance group, which oversees Sarbanes-Oxley compliance for Microsoft. She has held a similar role at another Fortune 500 company. She started her career with Deloitte & Touche in Seattle and has held many financial and operational leadership positions in the financial services industry, as well as in a number of start-up companies.

© 2006 ACM 1542-7730/06/0900 \$5.00