

Ask the expert How to: streamline regulatory compliance and audit

Srikant Sharma, Senior Director of Financial Services at Interwoven, explains

Sarbanes-Oxley (SOX) has disruptively elevated the importance and visibility of the internal controls function. In financial services, the relationship between internal audit and risk management is vitally important. Controls play a leading role in providing assurance that management is properly identifying and mitigating risks arising from business operations, internal systems and organizational structure. In other words, strong internal controls lead to a lower risk scoring, and hence, a lower level of regulatory intervention.

In order to provide proper oversight of enterprise risk, financial institutions must take a holistic view of risk and evolve internal controls processes to a higher level of automation. However, it is important to remember that optimizing internal controls cannot be successfully accomplished without first evaluating, thoroughly documenting and standardizing controls across the enterprise. It is this first step that provides the ability to measure controls effectiveness and continually improve and automate these processes. This is of paramount importance given the strict requirements the government has imposed to control financial risk within financial services organizations.

What prevents automation?

Although SOX has become a catalyst to implement a 'system of record' geared toward auditing the interaction between people, processes and content, multiple research firms report that the early lack of regulatory guidance regarding the role and relevance of IT has resulted in limited adoption of purpose-driven applications. As a result, much information remains fragmented, with content scattered in silos across the enterprise and in multiple contexts (such as text, documents, diagrams, test results and so on).

This fragmentation has contributed to significant control deficiencies. Ernst & Young, in their Emerging Trends in Internal Controls 2005 report, found that the majority of companies have only 20-40 percent of their controls automated. While manual controls are easier to understand and document, they are inherently less reliable and more labor-intensive to execute and test.

A contributing factor to these inefficiencies is the lack of a unified, enterprise-wide information management platform within many financial institutions. This underutilization of technology has come at a high cost for companies. The SEC, in 2005, noted that most organizations lacked a systematic judgment of which audit procedures were most important, resulting in the wrong controls being identified,

documented and tested. In addition, the lack of effective workflow and collaboration tools has resulted in poor coordination between external auditors and internal compliance teams, contributing to ineffective audit execution and sky-high external consulting fees.

This has resulted in less than desirable consequences: US banks have taken measures that are far beyond the original intent of regulators, yet many of these executives cannot effectively navigate their own organization in an era of increased accountability, where penalties for non-compliance are significant and can affect reputation and livelihood.

Content-based approach to automation

As financial institutions look to improve controls reliability, technology is becoming a key enabler of these efforts. According to research firm Forrester, a defined relationship exists between the maturity of internal controls processes and the use of enabling technology. The foundation for controls optimization and automation lies in a company's ability to achieve well-documented, standardized controls and to effectively manage the overall compliance process across the enterprise.

Collaborative content and document management systems are critical resources for achieving these goals. These compliance-driven applications provide workflow management that implements rules and role-based security models to assign, monitor, edit and sign off on assigned tasks across the entire organization. Multilevel user management significantly enhances preventive controls by providing and enforcing the proper segmentation of duties.

Equally important is the guaranteed integrity these technologies bring to the controls process by managing the compliance content lifecycle across the entire business. Sustainability is achieved through versioning features that provide complete audit trails. This means that each policy, procedure and control document within the enterprise has an explicit history and persistent identity when it is distributed throughout the organization and to external constituencies.

These same capabilities also allow individuals to safely collaborate on documents, regardless of their location. Information can be captured and distributed in a variety of formats, including text, process diagrams, questionnaires, spreadsheets and other documents to optimize their usability. Information is securely stored, managed and efficiently accessed from a centralized location to ensure the right information is available for reporting and analysis.

Monitoring and automation of internal control policies are attained through a number of software tools. Key capabilities within these tools are rule-based triggers that not only monitor, but can also help ensure compliance with corporate control policies as business processes occur. Triggers can be set at a variation of criteria such as dollar threshold, risk tolerance or organizational level to automate controls and eliminate errors as soon as they occur – eliminating cumbersome and error-prone manual audit procedures.

A complex combination

Compliance is complex and requires a combination of technologies that work in unison to effectively manage risk. There is no silver bullet, despite what many vendors would lead you to believe. Unfortunately, banks find themselves under increasing pressure to adopt 'flavor of the month' technologies, regardless of how well or poorly they integrate with established systems – increasing the probability that control deficiencies will be attributed to information systems. While compliance is the ultimate goal, bear in mind that these investments hold the potential to reap a positive and significant ROI through the avoidance of financial loss and improved operational efficiency.