

## Set Your Sights on Continuous Compliance

This article appeared in *“INNOVATION: The Convergence of Information Technology and Business,”* published by BMC Software.



To receive a copy of *INNOVATION: The Convergence of Information Technology and Business*, go to [www.bmc.com/innovation](http://www.bmc.com/innovation).



## Set Your Sights on Continuous Compliance

By David Greene

*Vice President, Solutions Marketing, BMC Software*

For multinational enterprises, the regulatory maze is getting more complex by the day. Each geography has its own set of governmental mandates and industry best practices. The effort required to comply with any given legislative act can be astronomical.

But what if compliance was just a result of how you run IT? Savvy IT professionals are discovering that developing compliance projects around specific legislation or the many personal data privacy regulations worldwide is not a viable approach. Instead, they are building a *continuous compliance* capability that provides a sustainable way to address changing government regulations, industry best practices, and internal corporate policies as part of the day-to-day preparation.

This approach takes into account the fact that the need for compliance doesn't go away once you've passed an audit. It's a continuous effort. If your organization typically takes a project-

based approach to government mandates, some rethinking of current projects can help you make the transition to a continuous compliance philosophy.

### **Taking a New Perspective**

If you've been operating in "project mode" to get through the next audit, it's time to change your perspective from "just complying with a mandate" to creating an enterprisewide program focusing on governance, risk, and compliance. So, if one of your highest-priority projects right now is preparing for a regulatory compliance audit, broaden your perspective. Clearly the project needs to focus on meeting the letter of the law. However, you should work toward reducing not only regulatory risk, but also operational risk. Moreover, your project should have a longer-term goal of reaching beyond compliance to improving your IT and operational processes and technology. That is, you should use compliance as a lever for business improvement.

For example, assume your company's key source of revenue comes from its online business. If your Web server goes down during manual maintenance tasks, your business can come to a screeching halt. To avoid this, consider establishing automated controls to manage changes to the servers that support online operations. Replacing tedious, manual controls with automated controls will more quickly satisfy auditors and can free up your staff to focus on innovative projects. It may also be the catalyst for reviewing your existing processes, such as those for change control, and determining how to streamline, simplify, and standardize them.

**You should work toward reducing not only regulatory risk, but also operational risk. Moreover, your project should have a longer-term goal of reaching beyond compliance to improving your IT and operational processes and technology. That is, you should use compliance as a lever for business improvement.**

You can also learn from past experience. Many organizations, for example, began their compliance initiatives by implementing more controls than they needed. The key is to try to reduce the number of controls. Just as an auditor's goal is to determine if a control set is sufficient, you should see where you can simplify and reduce your number of controls so you can manage them more effectively. By simplifying your approach, you can determine which controls do the job and which are excessive.



## Avoiding Common Control Deficiencies

The most common IT control deficiencies are based on improper change controls. Issues related to system documentation, which can become material weaknesses, are a symptom of inadequate controls. When documentation does not match the control processes that are used for changes, you cannot ensure that changes have been correctly authorized, approved, and tested.

A proactive approach involves automating IT controls, continuously monitoring their effectiveness, simplifying verification through reporting and monitoring, and enforcing control policies. That doesn't mean you need to buy a lot of new software. It simply means that you need to use the software you have more effectively and, by integrating processes properly, simplify the number of controls you have in place.

Automation is vital because most control problems start when changes are made. All too often, IT teams that rely on manual processes must sort through thousands of changes (documented in spreadsheets) to determine if the changes apply to the compliance project and, if so, whether or not they were input correctly. By using automated controls and monitoring their effectiveness, the IT organization can work more efficiently and, at the same time, reduce costs.

**A proactive approach involves automating IT controls, continuously monitoring their effectiveness, simplifying verification through reporting and monitoring, and enforcing control policies.**

Another common control deficiency relates to inadequate identification and tracking of IT assets and data. This is one area where a configuration management database (CMDB) works well. The IT Infrastructure Library (ITIL®) recommends that organizations use a CMDB to maintain information that defines the relationships between components in the IT environment and the business processes they support. A CMDB maintains the relationships among technology assets, processes, and people as configuration items. The CMDB should be supported by technology that incorporates ITIL best practices. It then becomes the centerpiece for process integration, a powerful way to extend the coverage of automated controls. With a CMDB, there are fewer controls to document, verify, and test. As a result, a well-architected CMDB can reduce the cost for compliance and associated risks.

Inadequate identity and access control is another deficiency frequently found during audits. Proper control can help companies avoid many long hours with auditors and eliminate the need to explain why terminated employees or former contractors still have access to your systems. According to Control Objectives for Information and related Technology (COBIT), a best-practice framework for IT governance, you should have a formal process for granting and revoking access privileges to systems and data. It's also important to periodically review and confirm access rights. An automated solution should provide a workflow capability to formally define and enforce the process for handling requests and approvals. The solution should also enable IT to manage and track the inevitable isolated requests that come through the system.

It's also essential to address issues related to segregation of duties — another significant IT control deficiency. Financial institutions have historically used segregation of duties as a checks-and-balances security method. For example, a person in charge of negotiating purchases with vendors should not be involved in the payment authorizations. This methodology is now mandated at an IT level. Identity management solutions can address this problem by restricting access and ensuring a secure audit trail. The information can then be correlated to access privileges and categorized based on the level of privileges.

An important consideration related to segregation of duties is the practice of allowing development staff to run business transactions in the production environment so they can gather information required for problem resolution. This uncontrolled access can violate governmental mandates and jeopardize data integrity and availability. Automated solutions can give developers the capabilities they need to solve problems without giving them direct access to production systems. This enhances the integrity and security of data and processes.

For more information about BMC solutions for compliance, visit [www.bmc.com/compliance](http://www.bmc.com/compliance).

### **Taking the Next Step**

The key to moving toward continuous compliance is a change in mindset. The new mindset embraces compliance as a sustainable process. This approach enables you to support not only the objectives of a particular government mandate, but also helps you run your IT organization more efficiently and flexibly, further advancing your company's growth and profits. This strategy will become even more valuable in the future as IT's role in compliance efforts continues to increase. Make compliance a part of how you do business in IT, and you will spend less time with auditors and more time running a better IT organization.

**About the Author**

*David Greene has more than 20 years of experience in technology marketing, along with considerable expertise in IT controls and professional services. As vice president of Solutions Marketing for BMC, he oversees the definition, positioning, and promotion of the vast portfolio of customer-focused solutions delivered by the company. Prior to joining BMC, Greene was vice president of Marketing and Professional Services at Active Reasoning. Greene also held management positions in marketing and IT at Hewlett-Packard. He has degrees in architecture and computer science from the University of California, Berkeley.*