

FIVE STEPS TO ACHIEVING A CONTINUOUSLY COMPLIANT DATA CENTER

By Vick Vaishnavi, vice president of Worldwide Marketing, BMC Software

What do you do when the “check engine” light comes on in your car while you are driving down the highway? Do you need to immediately pull over and call a tow truck? Probably not, but you should get the engine checked and the issue resolved as soon as possible. If you address it in a timely manner, it may be just a routine repair. However, if you ignore the light and keep driving day after day, you may cause serious damage to your engine, resulting in an expensive repair or replacement of engine components.

It's the same principle with data center compliance. Achieving and maintaining compliance with government regulations and industry standards can prevent a small issue from causing major damage to your company's financial well being or reputation due to security breaches and outages. These actions can apply to Sarbanes-Oxley 404, Statement on Auditing Standards (SAS) 70, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Basel II, and other regulations and standards.

Achieving and maintaining compliance can help your organization avoid the high cost of recovery and repair that goes along with unfavorable audit findings or having your business compromised. Some companies have had breaches that have resulted in losses of millions of dollars.

Just like what happens when automobile repairs are not done in a timely manner, costs can skyrocket when an infrastructure repair is performed too late. Industry estimates vary, but discovery, notification, and response costs alone related to a security breach are about \$50 per record. That figure doesn't

even include the cost of the negative impact on a company's brand and loss of customers. In fact, the cost of a breach can be anywhere from \$90 per record to more than \$300, depending on the type of breach and industry.¹

Now compare that with the cost of prevention — about \$16 per account to invest in technology and processes to support compliance. Automated processes and technology help to eliminate human error while improving efficiency and providing the needed IT controls.

Practicing continuous compliance is vital to ensuring credibility and profitability. It means having the right controls, knowing when people aren't following the rules, and finding out where and why this is happening. IT control deficiencies are the most costly and difficult ones to identify and, therefore, to bring into compliance. So the key is to focus on prevention. The best-practice approach described here provides a roadmap for achieving continuous compliance in the data center.

Step 1 — Definition and Goals

Start with your vision and a clear definition of compliance and the compliance goals you want to achieve. Specifically spelling out the definition and goals will ensure everyone is on the same page and will alleviate confusion and misunderstanding.

CREATING A COMPLIANCE DEFINITION

When you are defining what compliance means in your organization, be sure to address the following three facets: security, configuration assurance, and verification support.

Security involves patching, identifying vulnerabilities, and having access controls. From a security standpoint, compliance means ensuring that you have secured your servers and applications by keeping up to date with the latest patches. It means that you have identified vulnerabilities in the environment that require remediation, and have put appropriate access controls in place to limit administrative privileges. Patching, of course, helps eliminate vulnerabilities. Administrative privileges also need to be in place. Specifying who is authorized to perform various tasks on any given server at any given point in time protects systems from unauthorized access and helps you demonstrate compliance to auditors.

controls. These controls enable you to prove to an auditor, advisor, or regulator that your IT organization has the necessary mechanisms in place to meet the security and configuration facets. The regulatory piece also includes in-house audits to measure the effectiveness of your controls and ensures that you can pass external audits with ease.

ESTABLISHING COMPLIANCE GOALS

IT organizations that have achieved a high state of compliance have done so by setting and achieving four major goals: standardization, accountability, transparency, and measurability.

Standardization normalizes configuration settings across Windows, Linux, UNIX, and other platforms that comprise your infrastructure. Standards drive your build policies and help you identify risk.


Accountability is about establishing audit trails for the changes that have occurred, when they were implemented, who made them, and what impact the changes had on the environment. Through better accountability, you can ensure that only approved changes are made and that segregation-of-duties requirements are met. Good accountability also enhances IT management. It ensures that mechanisms are in place to alert you

when a system deviates from the norm, prompting you to take action to rectify the situation and to track down and eliminate the cause so that it doesn't happen again.

Transparency is primarily related to reporting; that is, gaining insight into what your people are doing. Reporting tells you what processes are in place to support compliance and how well they are functioning at any point of time. Transparency provides visibility to auditors so they can determine if your data center is compliant. You can assess your progress by answering

critical questions related to compliance, such as:

- » Did you experience fewer emergency changes this month than last month, six months ago, and last year at this time?
- » Has the drift from standards decreased over the past year?
- » Are some platforms, servers, applications, or business service servers more compliant than others? If so, why?



Start with your vision and a clear definition of compliance and the compliance goals you want to achieve.

Configuration comprises both establishing standard settings for all your systems and ensuring adherence to those standards. Merely putting in place standards, however, isn't enough. You must also define a process to monitor the environment and report on any services that drift from standards.

In defining the regulatory component, you create documentation, implementation, and verification of IT

Step 2 — Implementation

Automation is critical for ensuring continuous compliance with policy-based operations. There are three parts to the implementation step: choosing and implementing a governance framework, identifying and implementing controls, and adopting a platform to ensure continuous compliance.

IMPLEMENTING A GOVERNANCE FRAMEWORK

Follow the COBIT (Control Objectives for Information and related Technology) framework for guidance. COBIT's broad coverage means that you can leverage your investment to comply with multiple other regulations and standards, such as the Sarbanes-Oxley Act and Basel II. COBIT also integrates well with established frameworks, such as the Software Engineering Institute's Capability Maturity Model Integration (CMMI), ISO 20000, the IT Infrastructure Library® (ITIL®), and ISO 17799 (the standard security framework, which is now ISO 27000).

Following COBIT helps to reduce the cost of audits and self-assessments. It provides guidance for built-in support for IT audits, which enables managers to balance risk and control in a fast-changing IT environment. In addition, COBIT guidance assures users that their services and data are secure and provides auditors with substantiation for their opinions and evidence of control activities.

IDENTIFYING AND IMPLEMENTING CONTROLS

A phased approach with respect to implementing controls works best because you may need to address the many controls involved. Instead of trying to implement all of them at once, start with those required for a specific regulation or standard that you identified as a priority in Step 1. Alternatively, consider identifying "common denominators" — controls that will immediately bring you into compliance with multiple regulations. For example, related to access, change, release, and configuration controls will bring you into compliance with about 50 percent of today's regulations.

Regardless of your starting point, however, be sure to pay close attention to access controls. For example, one global financial services firm faced serious challenges with respect to access controls that disrupted its change process. Shared user IDs prevented IT from clearly identifying who had made each change, which can create a problem because only certain people are supposed to be able perform to specific changes. It became increasingly difficult for this organization to roll out changes to nearly 5,000 servers on a weekly basis, and using manual processes became overwhelming for the server administration staff.

By improving its access controls, the company was able to deliver substantial improvements to the change success rate and to staff productivity. The financial services provider used best-practice processes and automated tools around access, change, and release.

Adopting role-based access control enabled the security team to delegate the implementation of certain changes to groups requesting the change without impacting security. In the six years since the processes and tools were deployed and the issues related to shared IDs were resolved, the number of servers has increased five times and the number of applications has increased three times. The staff, however, has handled the increase with a dramatic improvement in the server-to-administrator ratio. The end result is that effective compliance enabled this IT organization to improve its business impact while simultaneously lowering risks and costs.

ADOPTING A COMPLIANCE PLATFORM

Your compliance platform can provide the foundation for the controls you implement. It should support three essential capabilities:

- » Prevention to keep unwanted events from happening
- » Detection to alert you immediately if problems have already happened that can impact compliance
- » Correction to automatically fix problems that have been detected

These capabilities will give you confidence that the IT controls you implement are working fully and delivering the level of compliance you need.

Step 3 — Measurement

Along with implementing the platform and controls, you need to put a mechanism in place to measure performance so that you can assess the effectiveness of the implementation. The specific metrics you choose will depend on your organization and the particular compliance objectives. Examples of metrics that many successful companies have leveraged include:

- » **Policy adherence** — What percent of the data center complies with each policy?
- » **Percentage of audit failures** — How significantly did you reduce the percentage of failed audits?
- » **Mean time to remediate** — How quickly can you fix a compliance issue that has been detected?
- » **Exceptions** — How significantly did you reduce the time required for detecting, documenting, and fixing exceptions?

When defining your metrics, make sure you limit your choices to things that you can effectively measure. Start with a small number of meaningful metrics and add to them only as necessary to increase transparency or adherence.

Step 4 — Enforcement

Maintaining continuous compliance is critical. Look at deviations to determine if they are more prevalent on a particular platform, role, or service. Investigating these areas guides you in applying resources to correct the deviations and ensuring that systems are always operating according to policy. Here's an example of how one company enforced compliance. A provider of broadband, television, phone, and mobile services had automated system-level and system-wide configuration changes and integrated them with approval processes. That helped the provider meet the credit card industry's PCI DSS (Payment Card Industry Data Security Standard) standard for monitoring ongoing compliance.

As a result of this automation, the company has improved management, control, and enforcement of configuration changes. The time required to deploy each configuration item is now 80 percent faster. In addition, the process has also improved data center stability and service quality, decreased application downtime, increased IT productivity, and reduced data center operating costs.

Step 5 — Monitoring

Monitoring is about providing insight into whether your environment is becoming more or less compliant and reporting any findings to management. It shows you how well controls are working and what activities are taking place. Management reports provide data for creating scorecards and identifying trends.

For example, a software as a service (SaaS) provider uses a combination of printed reports and dashboards to monitor compliance with a variety of regulatory requirements and industry standards, including PCI DSS, Statement on Auditing Standards (SAS) No. 70, and Sarbanes-Oxley. Reporting capabilities have made it very easy for the staff to show auditors the details of each change and the thoroughness of change control processes. According to staff members, demonstrating that current server configurations are all in compliance is effortless.

An Investment that Pays Off

Just as spending what's needed to keep your automobile in good repair will improve its overall value, making an investment to implement these best practices for a continuously compliant data center will ultimately improve the value of IT to the business. The effort you invest in these best practices will pay many dividends beyond compliance. To assist you in this effort, automated processes and tools help to eliminate human error, free up staff time, and bring greater stability to your IT infrastructure. All of these benefits can translate into lower costs, greater efficiency, and a good corporate image with customers — benefits that will position your company to compete more effectively now and when the economy rebounds.

For more information about BMC solutions to help maintain continuous compliance, visit www.bmc.com/bsm.

END NOTES

1. "Calculating the Cost of a Security Breach," Khalid Kark, Forrester Research, Inc., April 10, 2007.

ABOUT THE AUTHOR

Vick Vaishnavi, vice president of Worldwide Marketing for BMC Software, is responsible for driving BMC's global marketing strategy, market development, campaigns, and field operations activities.



He has 20 years of experience in enterprise IT software and has held executive and leadership roles in marketing, alliances development, product management, engineering, and sales operations at various companies, including BladeLogic, Rishisoft, Opticom, and APRISMA. Before joining BMC, he played a key role in transforming BladeLogic from its start-up stages to its successful acquisition by BMC. He has been awarded six United States and international patents for his work in IT management software systems. He holds a BSEE from IIT India, an MSCE from the University of Massachusetts, and an MBA in marketing and finance from Boston University School of Management.

BUSINESS RUNS ON I.T. I.T. RUNS ON BMC SOFTWARE

Business thrives when IT runs smarter, faster, and stronger. That's why the most demanding IT organizations in the world rely on BMC Software across both distributed and mainframe environments. Recognized as the leader in Business Service Management, BMC offers a comprehensive approach and unified platform that helps IT organizations cut cost, reduce risk, and drive business profit. For the four fiscal quarters ended March 31, 2009, BMC revenue was approximately \$1.87 billion. Visit www.bmc.com for more information.