

If Compliance Is So Critical, Why Are We Still Failing Audits?

How to Minimize Failure and Make the Audit Process Easier

By Alex Bakman

In one form or another, ensuring regulatory compliance serves as an important business and information technology (IT) objective for most organizations—and with good reason. The risks of noncompliance are real and tangible, from significant financial penalties to the threat of damage to an organization's reputation. Compounding the problem is the fact that the number of compliance regulations is growing; by some estimates, organizations will face twice as many compliance requirements by 2012 as they do now.

Given the obvious importance of compliance and the clear commitment most organizations have made to meeting regulatory requirements, why do so many organizations still fail their compliance audits? This concern is reinforced by a recent Verisign white paper, "Top Reasons Customers Fail PCI Audits," which stated that more than 73 percent of the customers surveyed admitted failing an audit.

Explanations for Failing Audits

Not surprisingly, given the number of compliance requirements and the evolving nature of the regulatory environment, one of the main reasons organizations fail during the audit process is a general lack of understanding of regulatory requirements and how to employ technical strategies that will mitigate IT risks. Even for the most prepared, it can be difficult to know exactly how requirements will be interpreted by auditors and which technologies will actually improve compliance efforts. Plus, it can be a challenge to know how to build frameworks to minimize the effort of complying with multiple, often overlapping, requirements.

A second reason organizations fail audits lies with the increased sophistication of auditors. Auditors, who have always had a thorough understanding of business operations in general, have now become more experienced in IT operations and are able to leverage this expertise when they evaluate an organization's compliance. At the same time, they are able to take advantage of more sophisticated automated tools to assess the level of compliance in the environments they are evaluating.

The third reason some organizations fail their audit is that they take an event-driven approach to compliance. In the face of increasing requirements and expectations for continuous compliance, it is essential for compliance initiatives to be strategic, integrated business processes and not one-time "projects." (See the evolution of compliance in **figure 1**.) It is no longer acceptable to be in compliance for "audits only." In fact, auditors are unlikely to accept manual, "one-off" compliance reports as auditable evidence and may even ask for information on a daily, weekly or yearly basis. This makes it important to

regularly evaluate the effectiveness of IT controls and compliance initiatives to ensure that goals are being met.

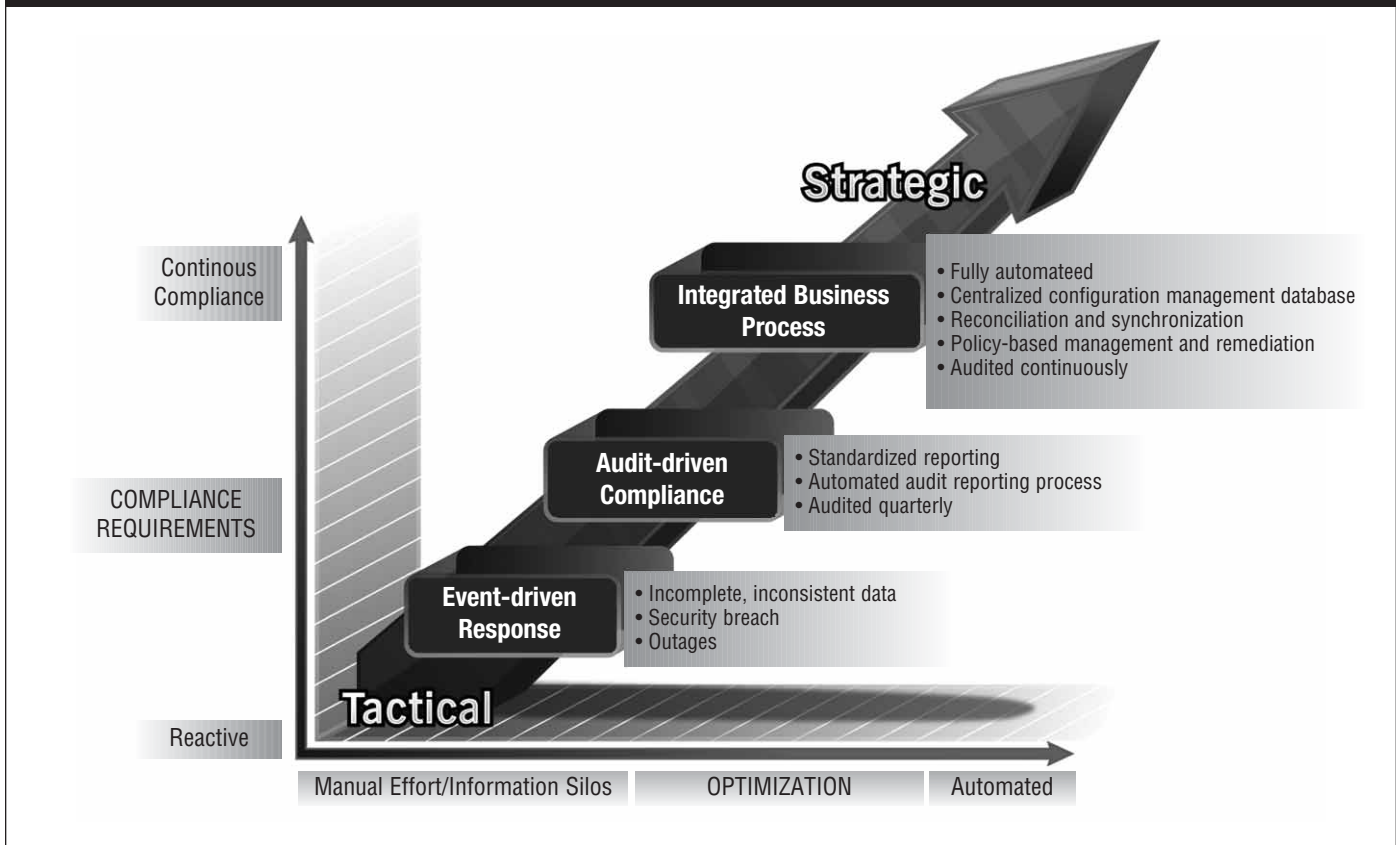
Finally, some organizations fail compliance audits because they lack comprehensive visibility into their infrastructure. According to Gartner, 50 to 80 percent of unplanned downtime is caused by people and process issues that result in unstable configuration changes.¹ A recent Enterprise Management Association report concurs, indicating that more than 60 percent of IT infrastructure problems are the direct result of change.² Without visibility into the organization—specifically at the configuration level—it is impossible to know whether an organization is compliant or deficient, or even where there are gaps between the two. To ensure continuous compliance, it is essential to ensure visibility at a very granular level.

Minimizing Failure and Making Audits Easier

While each one of the potential reasons for failing a compliance audit seems different on the surface, they can all be addressed with the implementation of a sustainable IT compliance program, which can be accomplished in four steps:

1. **Automate the IT control testing process.** By eliminating the human element of compliance, organizations can ensure consistency and preparedness, regardless of when an audit takes place. At the same time, automation enables organizations to redirect IT staff members toward other key IT initiatives. Plus, many auditors themselves are taking advantage of the automated tools at their disposal. According to the IT Policy Compliance Group's recent research report titled "Taking Action to Protect Sensitive Data," organizations with the fewest compliance problems spent 9 percent more to automate audit functions, but 11 percent less on contractors and outside services.³
2. **Validate the change management process.** Change management is a key component of the entire compliance process. IT controls evolve every time a change occurs in the infrastructure—whether for the deployment of new hardware or applications, the hiring of new personnel, or some other change—and auditors regularly evaluate the effectiveness of IT control and change management processes. When an organization can control and manage change on a continuous basis, it gains the visibility necessary to ensure that its infrastructures are secure, compliant and effective.
3. **Manage and minimize the list of IT controls.** With the implementation of the first compliance initiatives, many organizations sought to build a compliance framework by leveraging all of the control objectives of *Control Objectives*

Figure 1—Evolution of Compliance



for Information and related Technology (COBIT). It is now clear that, in some cases, this was too complex. To ensure successful audits, organizations should document all their controls and then minimize them to a list that is manageable and easy to understand. These controls should align with audit objectives and encompass only those that are critical to maintaining compliance. Once controls are established, a regular, proactive self-assessment of IT control processes can help organizations pinpoint problems as soon as they arise.

4. **Tackle the most material IT control gaps to ensure compliance.** In any organization, there will likely be compliance gaps, and it is important to focus on the gaps that could turn into a material weakness or cause an auditor to determine that an organization is not in compliance with a requirement.

A sustainable IT compliance program—and the associated IT controls and change management processes—can lead to additional benefits that should not be overlooked, including a more secure environment, improved operational efficiency and increased system performance.

Achieving IT Process Automation

There are six keys to successfully implementing IT process automation. These keys include discovering, collecting, reporting, analyzing, validating and remediating critical configuration data (see figure 2).

Discover

In the discover phase, organizations should use an automated approach to identify and classify all systems in the environment in a complete inventory, particularly those that are critical in the scope of compliance requirements. As an added benefit, a comprehensive inventory will pinpoint any rogue systems in the environment, increasing security.

In this phase, organizations should take the following steps:

- Use autodiscovery to save time finding systems.
- Keep an accurate enterprise inventory.
- Use a variety of discovery approaches.
- Prevent rogue systems from going undetected in the organization's environment.

Collect

For increased visibility into the environment, organizations should collect data from across the infrastructure and use that data to populate a centralized change management database. The preferred approach is to use an agentless solution that does not rely on software deployed on targeted systems. A noninvasive solution eliminates the need for agents that can slow down the system or introduce additional problems.

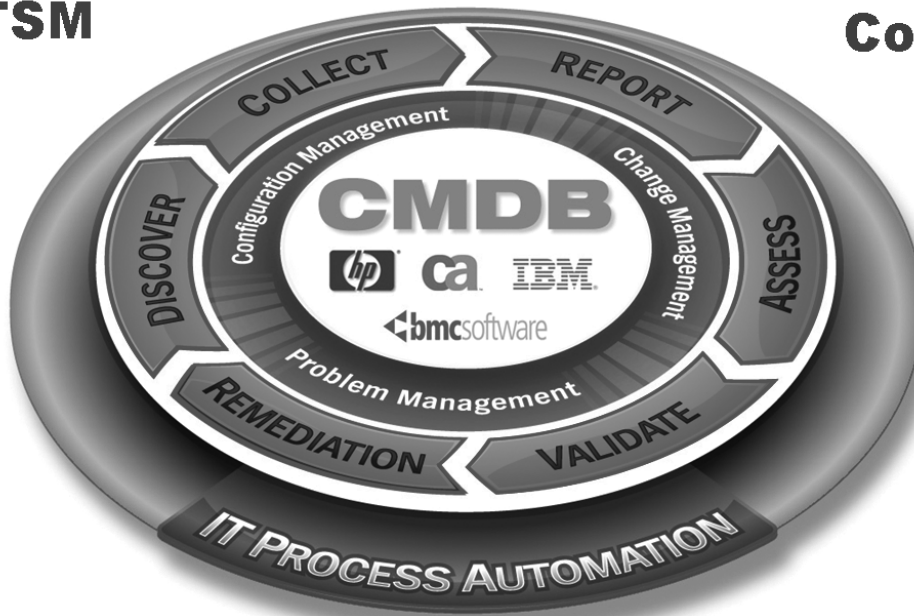
Organizations should take the following steps in the collect phase:

- Collect from the entire environment (operating systems, applications, mail servers, directory services network devices, etc.), as only a broad view provides accurate reporting.

Figure 2—IT Process Automation Wheel

ITSM

Compliance



- Use data to populate a centralized configuration management database (CMDB).

Report

To report on the results of discovery and collection, organizations can look to audit-ready reports from solutions that can help streamline the audit process. A general lack of understanding of compliance requirements is one of the reasons many organizations fail audits. Reports tailored to address specific compliance requirements can take the guesswork out of the compliance process, as they reduce the workload of frequently strapped IT teams. Plus, automated reports that come directly from IT systems can become auditable evidence, and can be delivered to the auditor at the start of the audit process.

In the report phase, organizations should complete the following steps:

- Take advantage of audit-ready report templates to save time researching and interpreting compliance laws.
- Schedule automated reporting to reduce staff workload.
- Use automated reports to complete a preaudit so misconfigurations can be corrected.
- Look to automated report templates as an immediate deliverable for the auditor, to greatly reduce audit length and cost.

Analyze

The analyze phase begins with predefined policies and rules that align with compliance regulations. Successful data analysis must be conducted within the scope of a clear security policy, so organizations should begin any IT compliance process by ensuring that a comprehensive security policy is in place. In fact, IT controls evolve from the security policy as well.

In this phase, organizations should complete the following steps:

- Ensure that a clear security policy is in place.
- Look to technology solutions that have predefined policies and rules for compliance regulations and leading information security standards.
- Use dashboards to gain an at-a-glance assessment of policy compliance.

Validate

An effective change management process and visibility into configuration changes are integral to a successful IT compliance program. To validate results, it is important to confirm that the change management process has been followed and is working effectively.

Organizations should perform the following steps in the validate phase:

- Confirm that the change management process is being followed.
- Validate configuration and security policies.
- Use dashboards to show compliance against policies.
- Use preloaded report templates as deliverables for auditors.

In both the analyze and validate phases, taking advantage of dashboards can help organizations—and executives at all levels—maintain continuous visibility into compliance status.

Remediate

The remediate step is part of the documentation process and helps organizations pinpoint what must be changed within the infrastructure to ensure compliance. The remediation step can also be helpful during preaudit assessment to correct problems before the audit actually takes place.

In this phase, organizations should complete the following steps:

- Know what to change with exception reports.
- Use a web-accessible dashboard to identify problems to the attribute level.

A Sustainable, Automated IT Compliance Program

The answer for organizations struggling in the face of failed compliance audits lies in a sustainable, automated IT compliance program. With this approach, organizations can deliver the auditable evidence auditors need, increasing the reliability of the process from the auditor's point of view. At the same time, they ensure their capability to validate compliance over time with a systematic approach to ensuring compliance on the IT infrastructure.

Endnotes

- ¹ Scott, Donna; "Making Smart Investments to Reduce Unplanned Downtime," Gartner
- ² Enterprise Management Associates Inc., EMA Product Brief, 2007
- ³ Greenemeier, Larry; *InformationWeek*, 2006

Alex Bakman

is chairman and founder of Ecora, a software company that has helped more than 3,500 organizations worldwide meet their regulatory compliance requirements. His expertise is in IT security, audit and compliance, and he has been recognized with the award of patents in Israel, the US and the UK for his pioneering role in automating the identification and reporting of systemwide configuration settings. He is a frequent speaker at ISACA and Institute for Internal Auditors conferences. He is also a published author, with articles appearing in publications such as *Computerworld*. His experience as director of IT for a *Fortune* 500 insurance company adds real-world perspective to his understanding of the challenges facing today's IT executives.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2007 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org