



Prevention, Detection, and Investigation:
A Practical Approach for Activating Continuous Compliance

Table of Contents

- Executive Summary 1

- Meeting Compliance Objectives: Year One, Year Two, and Beyond..... 2
 - > Year One..... 2
 - > Year Two and Beyond 2

- Prevent, Detect, and Investigate (PDI)..... 3
 - > Taking Corrective Action..... 4
 - > Prevent: Who authorized what?..... 4
 - > Detect: Who has access to what?..... 4
 - > Investigate: Who did what? 5

- PDI and Closed-loop Client Management 5

- BMC Identity Management On-Demand Managed Service..... 6

- Conclusion..... 6

Executive Summary

Today's businesses are faced with a "compliance" tidal wave, a rising flood of regulatory mandates and control frameworks that are increasing both in breadth and depth. As the first signs of this wave approached, and deadlines for specific compliance objectives loomed, many organizations viewed their initial compliance initiatives as one-off tasks — projects to be planned, executed, and completed by the deadline.

It became apparent that this first wave of regulatory mandates was not an isolated occurrence, but a harbinger of the steady flow of external and internal compliance requirements that were to come, including Sarbanes-Oxley, HIPAA, PCI, GLBA, FFIEC, and Basel II, among others. Forward-looking organizations started to seek out practical ways to address not only current compliance needs, but future needs, as well, by creating a platform broad enough to capture the full scope of the wave.

Businesses are achieving this state of continuous compliance by integrating audit and control activities into business processes. Compliance is ultimately about assigning responsibility — all the way down to an individual person. As a result, identity management is the most logical place to start for many organizations.

This paper describes a practical approach for activating continuous compliance based on best practices of prevention, detection, and investigation, enabled by effective identity management. BMC® Identity Management solutions not only enable you prevent, detect, and investigate audit issues in a continuous and consistent manner, but they also transform static audit data into actionable, corrective opportunities, allowing your compliance infrastructure to evolve in tandem with your dynamic business environment.

Meeting Compliance Objectives: Year One, Year Two, and Beyond

Year One

The compliance storm for many businesses began in what has become known as “year one,” or the first year of compliance with Sarbanes-Oxley. Faced with a hard deadline, management typically treated the challenge as if it were a project, and adopted the mantra of “just get it done.” To clear this initial hurdle, businesses spent millions of dollars and booked countless hours of auditor, employee, and consultant time.

What was the result? The audits were completed; compliance was demonstrated to a minimum level of satisfaction; and the organization was left with scores of newly created, manual control processes that continued to sink untold hours of productivity.

Year Two and Beyond

Once the aftershock had passed and organizations had a chance to take stock of their situations, they soon realized that audits would be needed again shortly, and compliance had to be demonstrated once more.

One-time budget expenditures that organizations had set aside for the “compliance project” would need to be made again — and again. In addition, it was clear that something had to be done about the stopgap manual processes that were draining productivity.

The mantra for year two and beyond has become “automate and optimize” — compliance efforts must make the leap from project to process. The challenge has moved beyond trying to create the control processes needed to demonstrate compliance, and now lies in finding the right combination of framework and tools to transform compliance measures into a business process that can be automated and optimized.

A practical “Prevent, Detect, and Investigate (PDI)” approach provides guidelines for automating and optimizing control activities in a way that integrates with existing business processes, enabling you to activate continuous compliance. From its roots as a set of best practices adopted by organizations that were consistently effective at demonstrating compliance, PDI has evolved into a method for efficiently mapping the control and compliance activities you perform everyday to your IT control infrastructure; that is, the tools you have to do the job.

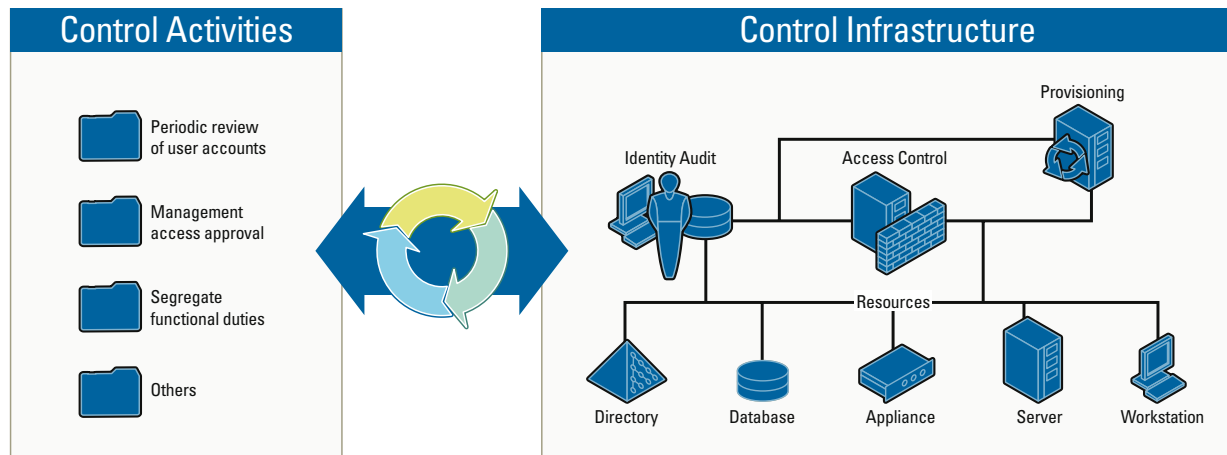


Figure 1. PDI is an approach for mapping control activities to control infrastructure

Prevent, Detect, and Investigate (PDI)

While each regulatory mandate and control framework typically defines its own requirements, they all ultimately seek to assign responsibility within business processes. This assignment of responsibility manifests itself as a set of control objectives (such as protecting data integrity and confidentiality) that are ultimately distilled into a core set of control activities. It is these control activities, the everyday actions that are currently being accomplished through manual processes, that you must automate and optimize to activate continuous compliance.

You can picture the situation in this way: On one side you have control activities, such as periodic reviews of user accounts, management access approval, and segregation of functional duties. These tasks are defined by managers and auditors as being necessary to perform on a regular basis to demonstrate fulfillment of control objectives that satisfy compliance regulations. On the other side, you have an IT control infrastructure: the servers, applications, systems, and tools you use to perform the control activities.

PDI is an approach that links the control activities that demonstrate compliance with your existing IT control infrastructure to enable optimization and automation. PDI accomplishes this by leveraging effective identity management to help you consistently and continuously answer three fundamental questions:

- > Who authorized what?
- > Who has access to what?
- > Who did what?

In short, PDI is about creating a sustainable, integrated approach that helps you prevent potential compliance and regulatory conflicts you know about; detect changes in your security and access environment that may compromise compliance; and investigate the activities that you previously did not know to prevent or detect. This cycle allows you to build a compliance infrastructure that evolves and continuously adapts to your constantly changing external regulatory requirements and internal organizational environments.

Controlling Developer Access to Production

One of the most intractable problems for businesses with in-house development teams is limiting developer access to the production environment. To avoid "separation of duties" conflicts, businesses must limit developer access to production systems. However, in order to enable rapid repairs or updates to applications in production, businesses typically grant developers broad access rights. For many organizations caught in this dilemma, there has been little that could be done, other than hope the developers were not installing Trojan horses or performing any other malicious actions.

BMC® AppSight™ Application Problem Resolution System (BMC AppSight) solves the developer access to production problem by inserting a black box between the developers and production. BMC AppSight records how the system works and behaves, and serves as the only interface between developers and the production environment. Developers can test out and implement fixes in the black box environment, which BMC AppSight will then apply to production. As a result, developers do not need, and are not granted, access to production systems.

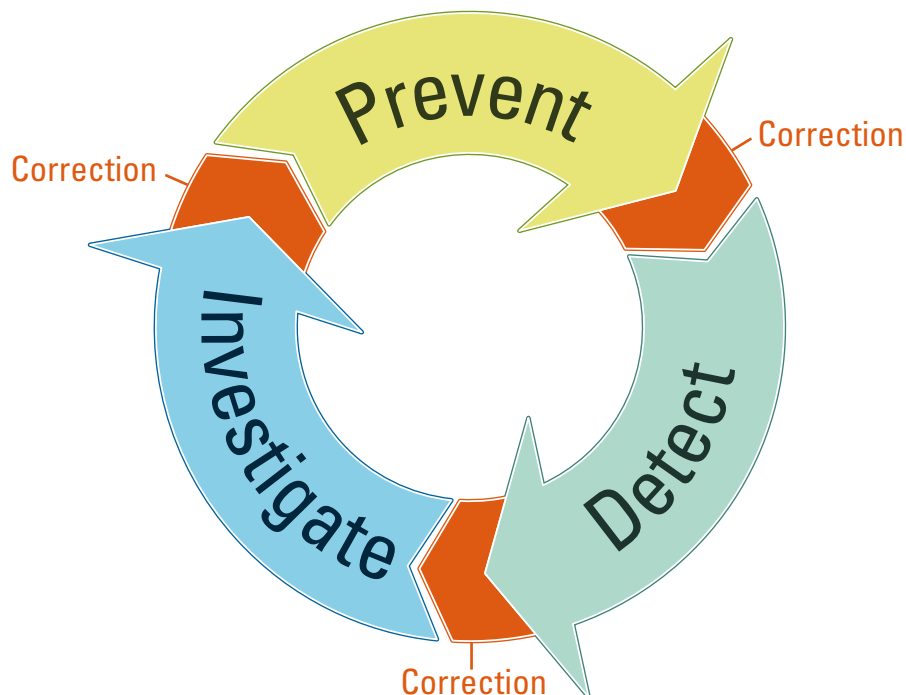


Figure 2. Opportunities for corrective action throughout the PDI cycle

Taking Corrective Action

At each stage of the PDI cycle there is an opportunity to take corrective action and enable continuous improvement. With PDI, you not only have the ability to report on identity audit information, but also the ability to transform this information into actionable correction opportunities. These corrections are essential for your compliance efforts to evolve in step with a dynamic business environment. For example, an integrated set of core identity management functionality, combined with a consistent workflow, enables you to use information obtained in investigative audits to update and improve your organization's prevention and detection mechanisms.

Prevent: Who authorized what?

Perhaps one of the most difficult challenges of any compliance effort is preventing compliance issues from occurring in the first place, starting with the assignment or authorization of appropriate access rights. In many organizations, this process is fractured, spanning multiple departments and approvers (both technical and line of business). The result is too often a process marked by spotty documentation, questionable accuracy, and insufficient accountability. The wasted time and resources consumed by such manual, error-prone processes are reason enough to rethink this approach to assigning access — but audit standards and regulatory requirements demand it.

So where to begin? Ideally, the assignment of appropriate access rights should be performed by the party that best understands the nature of the work. In most cases, this is the business manager. As an organization, you can only prevent actions that are already within your understanding of security possibilities or compliance activity requirements.

For example, your organization relies on a manager in the initial hire process to realize that the new hire has a specific role for which the organization has currently defined a set of rules.

As another example, consider the control activity for avoiding "separation of duties" conflicts. This control activity is central to many control and compliance frameworks. At a basic level, there are some things that specific groups of employees should be able to access that others should not to avoid conflicts of interest. A common case is the accounts receivable and accounts payable groups. As a business, you generally do not want someone who has the authority to both generate an invoice and cut a check to pay that invoice.

Separation of duties is an example of a prevention activity automated by identity management. This is accomplished by linking a workflow-automated business process to user provisioning. BMC Identity Management automatically provisions the appropriate access rights to systems based on a new hire's role and responsibilities within the organization, as determined by the business manager. The manager who decides what systems and access rights are assigned to a person in a particular role prevents a "separation of duties" conflict.

Further, should such a conflict arise, BMC Identity Management enables the manager to see the conflict, and take corrective action — for example by automatically notifying the appropriate business managers, allowing them to approve or reject the conflict, and removing access to one or more systems — all the while documenting every step, recording who made the authorizations, and generating audit trails that satisfy auditors and regulators.

Detect: Who has access to what?

In PDI, detection will catch the compliance issues that are still within your organizational understanding of a particular framework. These are situations that may arise as a result of insufficient control mechanisms for a specific change, such as a change in roles within the company. Similarly, they may arise after a re-organization or other business change.

In the "separation of duties" example, the accounts payable clerk was initially prevented from having access to accounts receivable systems. Later, that clerk may take a new position in accounts receivable. Without adequate control mechanisms to review access rights or detect the change of roles, the "separation of duties" conflict appears. Once again, business managers can use BMC Identity Management to automatically detect such conflicts and resolve them through a review cycle that identifies known issues.

Attestation and recertification of employees also highlights the importance of effective detection. For Sarbanes-Oxley compliance, when companies' CEOs sign the annual financial statement certifying that they know the information to be accurate, they are implicitly stating that they know the right people had access to the right systems at the right time to prepare the report. In any reasonably large organization, it is impossible for the CEO to have direct knowledge that every employee has appropriate access to the right systems. While the CEO may not be able to attest or certify that a particular accounts payable clerk's access is correct, that clerk's direct manager can, using BMC Identity Management.

During recertification, BMC Identity Management helps automate the recertification and the detection of policy violations. For each member of his or her staff, the manager can easily recertify the employee, revoke access rights, or forward the case to an appropriate administrator. The evaluation of access rights is delegated to the appropriate level and the workflow is automated to optimize the control activity.

Each issue that is detected during recertification or other review cycles presents an opportunity for correction, enabling the organization to improve its preventative policies and mechanisms to keep the problem from occurring in the same way again.

Investigate: Who did what?

Even organizations with mature and comprehensive control frameworks will not be able to prevent — or even readily detect — all compliance issues. Some problems may be beyond the scope of normal control parameters, or may reflect a breach of control parameters that have been previously established.

In order to investigate effectively, you must have an identity management infrastructure in place that accurately logs each approval, access, and authorization. This documentation enables you to answer the question, “Who did what?”

Gathering adequate and relevant information about identity and access activity is a common problem faced by many organizations, particularly those in the healthcare industry. Compliance with HIPAA regulations (among others) requires strictly controlled access to confidential data. With PDI and BMC Identity Management solutions, you can precisely limit access to specific systems within predetermined timeframes. More importantly, you can gather the information needed to monitor user activity and investigate it. BMC solutions enable you to perform user monitoring control activities in a practical way, while also providing the access your employees need to do their jobs.

Problems discovered through investigation are clear opportunities for improving prevention and detection. Organizations can guard against previously unanticipated actions or scenarios by adjusting policies and establishing detection mechanisms that will discover similar problems during scheduled reviews.

PDI and Closed-loop Client Management

As an example of how PDI provides a practical approach for activating continuous compliance, let's examine a use case of BMC solutions for Closed-loop Client Management.

In this example, a new employee is about to begin work and needs a laptop computer and access to business systems. BMC Closed-loop Client Management automatically provisions that employee with an appropriately configured machine and access rights, reducing the expenses and delays associated with manual processes. More importantly from a compliance perspective, BMC solutions ensure full control and auditability of all changes.

Here are the high-level steps:

1) When the new employee is entered into the HR system, the system triggers BMC Identity Management into action. BMC Identity Management enters the new employee into the appropriate user groups in the BMC® Atrium™ Configuration Management Database (CMDB), depending

on that employee's job role. BMC Identity Management then opens a request for change (RFC) in BMC® Remedy® Service Desk to provision the new employee. BMC Remedy Service Desk logs the RFC and forwards it to BMC® Remedy® Change Management.

2) BMC Remedy Change Management automatically routes the change request for approval. Also at this time, the asset management staff, using BMC® Remedy® Asset Management, checks the availability of an appropriate laptop and sufficient software licenses in inventory, and assigns a laptop from inventory. In addition, BMC Identity Management provisions the client with user IDs and passwords to the appropriate enterprise applications, based on the employee's role. In this step, compliance violations are prevented by following established policies for separation of duties.

3) When all required approvals have been gathered, BMC Remedy Change Management automatically generates a change ticket. It builds the ticket automatically from a predefined new employee template that is based on the user groups in the BMC Atrium CMDB into which BMC Identity Management has placed the new employee. The template specifies the software configuration to be provisioned to that employee's machine. The template also includes a predefined task list that BMC Remedy Change Management passes via data integration to BMC® Configuration Manager for Clients for implementation.

4) BMC Configuration Manager for Clients manages the execution of the provisioning tasks. It automatically deploys the appropriate application stack and content to the employee's laptop from the BMC® Definitive Software Library (DSL). BMC Configuration Manager for Clients then verifies the successful provisioning of the new laptop and notifies BMC Remedy Change Management when successful verification is completed. BMC Remedy Change Management closes the initiating change request and notifies BMC Remedy Service Desk of successful provisioning, closing the loop.

5) Upon reconciling the next discovery scan into the BMC Atrium CMDB (using BMC® Discovery solutions), newly discovered applications or versions to software license contracts in BMC Remedy Asset Management are matched via the DSL, keeping track of license compliance.

Along the way, all approvals and authorizations are logged, enabling effective detection and investigation of compliance exceptions in the future. Along the way, all approvals and authorizations are logged, enabling effective detection and investigation of compliance exceptions in the future.

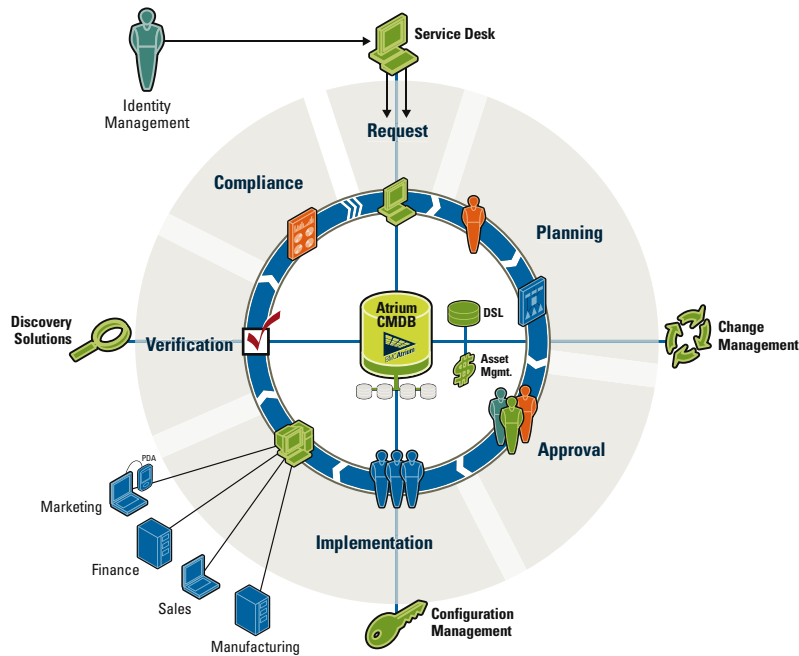


Figure 3. Closed-loop Client Management

BMC® Identity Management On-Demand Managed Service

Today's dynamic business environment means that organizations must find the mix of software and services that best aligns with their core competencies and resources. To help our customers meet this challenge, BMC has enhanced its identity management offering to include the BMC Identity Management Managed Service. This service combines BMC® Identity Management software solutions with the best-practice processes and in-depth expertise of service provider partners to rapidly enable PDI.

The service includes:

- > Highly standardized best-practice deployment
- > Hosting in your data center — all hardware and software delivered
- > Ongoing administration and maintenance of the bundled BMC and third-party technology used for the service

Conclusion

To successfully navigate the flood of existing and new regulatory requirements, your business needs a practical way to map control activities to its IT control infrastructure.

PDI, supported by BMC Identity Management solutions, enables you to activate continuous compliance by addressing compliance not as a project, but as part of your business process. PDI provides you with a comprehensive way to automate and optimize your compliance processes by setting and enforcing preventative policies, detecting exceptions to them, and logging and analyzing information to investigate problems. Throughout the process, PDI offers opportunities to take corrective action, enabling your compliance efforts to evolve to meet the needs of your dynamic business environment.



ACTIVATE BUSINESS WITH THE POWER OF I.T.™

About BMC Software

BMC Software delivers the solutions IT needs to increase business value through better management of technology and IT processes. Our industry-leading Business Service Management solutions help you reduce cost, lower risk of business disruption, and benefit from an IT infrastructure built to support business growth and flexibility. Only BMC provides best practice IT processes, automated technology management, and award-winning BMC® Atrium™ technologies that offer a shared view into how IT services support business priorities. Known for enterprise solutions that span mainframe, distributed systems, and end-user devices, BMC also delivers solutions that address the unique challenges of the mid-sized business. Founded in 1980, BMC has offices worldwide and fiscal 2006 revenues of more than \$1.49 billion. Activate your business with the power of IT. www.bmc.com.

