



Meeting the Challenge of IT Security Compliance in the Federal Government

How IT Organizations in Federal Government Agencies Can Achieve
and Maintain Compliance with Security Regulations and Standards

TABLE OF CONTENTS

- EXECUTIVE SUMMARY 1

- THE COMPLIANCE CHALLENGE 2
 - » Periodic Auditing Is Costly and Insufficient 2
 - » Security Responsibilities Are Divided 2

- FROM PERIODIC EVENTS TO EVERYDAY CULTURE. 3
 - » Implement Repeatable Processes Based on Best Practices 3
 - » Integrate Processes 3
 - » Provide a Comprehensive and Consistent View of the IT Ecosystem 3
 - » Implement Effective Change Management. 4
 - » Automate Processes 4
 - » Facilitate Compliance Testing. 4
 - » Foster Collaboration Between IT and Security. 4

- BSM SOLUTION CRITERIA 5
 - » Implement and Integrate Best-Practice Processes. 5
 - » Build on a Well-Architected CMDB 5
 - » Support End-to-End Change Processes 5
 - » Provide Comprehensive, Policy-Based Automation 5

- THE RESULTS SPEAK FOR THEMSELVES 6
 - » Some Organizations Are Already Enjoying the Advantages. 6

- CONCLUSION 7

- APPENDIX 8

EXECUTIVE SUMMARY

The United States government must process and protect vast amounts of data essential to our country's welfare. The challenge for government IT organizations is to make this information available when and where it is needed, without risking the security of that data or the government's networks. Compromising sensitive information could result in serious consequences, ranging from privacy issues, to public embarrassment, to compromised national security.

To ensure the necessary level of security, IT organizations must maintain and demonstrate compliance with a large and growing number of IT operational and governance regulations, policies, and standards. Attaining consistent and continual compliance presents significant challenges, especially considering the complexity of the IT environments in most agencies and the budgetary constraints.

The implementation and enforcement of repeatable, sustainable processes are critical to the success of government IT organizations. Business Service Management (BSM) solutions are available to help achieve these objectives. BSM is a comprehensive approach and unified platform for running IT according to business priorities. With BSM solutions and processes in place, you can attain consistent and continual compliance while reducing compliance costs.

This paper does the following:

- » Reviews the key security regulations that federal IT organizations face and describes the challenge of maintaining and demonstrating compliance with them
- » Presents an approach for creating a culture that integrates security and compliance into the day-to-day operations of the IT organization
- » Discusses how BSM solutions can support the approach by implementing and automating best-practice IT processes, such as those outlined in the IT Infrastructure Library® (ITIL®)
- » Describes the criteria that BSM solutions must meet to support the approach effectively
- » Presents the resulting business benefits and some real-world examples of federal agencies that have successfully employed the approach

THE COMPLIANCE CHALLENGE

IT organizations in the federal government must maintain and demonstrate compliance with a complex array of regulatory frameworks, security standards, and guidelines. While many different regulatory standards must be addressed by different agencies that have diverse missions,¹ the most important and overarching standard is the Federal Information Security Management Act of 2002 (FISMA). This act requires each federal agency to develop, document, and implement cost-effective programs to achieve information security on their systems.

The National Institute of Standards and Technology (NIST) has been tasked with “[promoting] the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act.” In support of this mission, NIST has organized standards from various public and private sources,² including:

- » Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
- » National Security Agency/Central Security Service (NSA/CSS) Security Guides
- » Center for Internet Security (CIS) Benchmarks
- » Federal Desktop Core Configuration (FDCC)

Thanks to the efforts of NIST, federal agencies will have fewer problems finding an appropriate set of standards for their environments. The IT organizations in those agencies, however, still face enormous costs and difficulties in the implementation of those standards.

PERIODIC AUDITING IS COSTLY AND INSUFFICIENT

Preparing for compliance auditing can be time consuming and expensive. Auditors require detailed reports that show that the organization is in compliance with all applicable laws and standards, that all IT assets are in compliance with configuration standards, and that only approved software is deployed. If any noncompliance issues surface, IT must provide the details for their remediation.

The processes for data gathering, reporting, and remediation in preparation for an audit are often manual and not well documented, making them labor intensive, inconsistent, and error prone. The job is further complicated when the data is fragmented across siloed IT groups, each with only a partial view of the IT infrastructure. In some cases, these groups have conflicting or unreliable information, making data consolidation even more difficult.

As a result, auditing is a high-cost, high-effort activity. Periodic compliance auditing alone, however, does not ensure the continued confidentiality, integrity, and availability of agency information. Compliance must be maintained on an ongoing basis, not just during audits. This long-term endeavor requires additional effort and processes, many of which are manual, undocumented, and fragmented across siloed groups. The inevitable end result is additional time-consuming and inconsistent process execution, driving costs up even higher, while still exposing the organization to the risk of noncompliance.

SECURITY RESPONSIBILITIES ARE DIVIDED

Another challenge facing IT organizations is that security responsibilities typically are divided between IT and a security group that might be outside the IT organization. The security group supports compliance audits and establishes policies to ensure that IT meets the regulatory requirements for security. IT must operate, maintain, and support the IT ecosystem to comply with these policies.

The separation of the two groups makes it difficult to achieve the close collaboration necessary to enable IT to fully understand and effectively implement the policies mandated by the security group and to enable the security group to effectively monitor IT’s compliance with these policies.

FROM PERIODIC EVENTS TO EVERYDAY CULTURE

To meet the challenges of compliance, you must make compliance an integral part of the everyday culture rather than a once-a-year audit event. You'll need to develop a number of capabilities that enable your IT organization to monitor and maintain compliance with all relevant regulations and standards on an ongoing basis. These capabilities are described in the sections that follow.

IMPLEMENT REPEATABLE PROCESSES BASED ON BEST PRACTICES

It's important to implement, document, and enforce repeatable processes, including the following:

- » **Configuration management** processes to ensure that only compliant configurations are deployed and maintained across the IT infrastructure
- » **Change management** processes to ensure that all changes are requested, planned, approved, implemented, verified, and documented according to compliance requirements
- » **Incident and problem management** processes to ensure that all compliance-related issues are detected and remediated expeditiously

These processes should be based on proven best practices, and they should be documented and tested against policies to ensure the policies are enforced. In addition, the processes should be integrated across silos and should be in compliance with relevant standards.

To meet these requirements, many federal agency IT organizations are turning to ITIL — a comprehensive framework of guidelines for implementing best-practice processes across all IT disciplines. Many of the ITIL processes strongly support mandated standards, including FISMA-based policies such as NIST SP 800-53. What's more, ITIL processes align tightly with the IT governance guidelines outlined in the Control Objectives for Information and related Technology (COBIT) framework. COBIT, in turn, aligns with the controls specified in NIST SP 800-53.

INTEGRATE PROCESSES

Process integration is key to ITIL and is important even if you are not implementing ITIL best practices. Integrating processes across IT disciplines and between IT and the security group enables seamless workflow and facilitates collaboration among groups so that processes run smoothly and key steps are not overlooked. Here are some examples:

- » Integrating compliance testing with incident and problem management ensures that out-of-compliance issues are addressed in a timely fashion. This integration also provides insight to the incident and problem management team to facilitate remediation.
- » Integrating incident and problem management with change management ensures that your team implements all requested compliance-related fixes according to a change policy that adheres to compliance requirements. This minimizes the risk of a remediation change introducing additional compliance issues, and it ensures that all changes are properly documented to meet compliance audit requirements.
- » Integrating change management with configuration management ensures that only configurations that comply with configuration standards such as STIGs are deployed and maintained.

PROVIDE A COMPREHENSIVE AND CONSISTENT VIEW OF THE I.T. ECOSYSTEM

A single, comprehensive, and accurate view of the IT ecosystem enables all groups in your agency's IT organization to effectively monitor and manage compliance on an ongoing basis. That view must show all assets — physical and virtual, as well as main-frame and distributed — along with asset configurations and maps of the physical and logical asset dependencies. The view must also show the relationships of the assets to the services they support and a log of all relevant incidents and changes to assets. In addition, the view should show IT projects, people, and vendors and their relationships to the assets.

This single, comprehensive view gives all of the agency's IT groups greater insight into the root causes and scope of compliance issues, enabling faster remediation. In addition, through a better understanding of services and their underlying infrastructure, the IT staff can prioritize critical compliance issues to minimize their impact.

IMPLEMENT EFFECTIVE CHANGE MANAGEMENT

It's a well-known fact that improperly managed changes are a major source of noncompliance issues and service disruption, and federal agencies are no exception. Alleviating this problem requires effective governance of the entire change process, including the following:

- » **Planning** — Determine up front the impact of proposed changes; for example, to help assess risk, you should identify the assets involved and the services they support.
- » **Authorization** — Set up controls to ensure that changes can be requested only by authorized personnel and that all changes are properly approved before execution.
- » **Implementation** — Ensure that only authorized changes are implemented and that only authorized personnel implement changes.
- » **Documentation** — For every change, maintain a record of what change was made, when it was made, who made it, and who authorized it.

Change governance must encompass all changes to the IT environment, including changes made to ensure disaster recovery and continuity of operations. In addition, you must be able to quickly detect the occurrence of unauthorized changes, assess their compliance impact, and remediate them accordingly.

AUTOMATE PROCESSES

Policy-based automation ensures that processes are always performed in a manner consistent with compliance requirements. IT organizations should strive to automate manual processes wherever possible. Automation eliminates reliance on highly skilled staff, and it helps reduce workload so you can cut costs. Automation also streamlines workflow within and across IT groups. Here's an example of how a solution with policy-based automation delivers these benefits:

The IT staff needs to implement a critical security update to hundreds of servers located throughout the agency's data centers. The solution facilitates the generation of the change request by automatically populating known entries. It enables the staff to quickly pretest server configurations to validate that they can accommodate the update. The solution automatically gathers the required change approvals, triggers the change implementation, and distributes and installs the update. It verifies successful installation and generates incident tickets for any servers not successfully updated. In addition, the solution tracks all processes, records the information required for audits, and provides status updates to personnel affected by the change.

FACILITATE COMPLIANCE TESTING

It is essential to continually monitor the IT environment for compliance with security policies. Because of the size and complexity of federal agency IT environments, manual compliance testing is not practical. You can achieve cost-effective compliance testing by automating the testing of assets to implemented policies. Through automation, insecure configurations can be quickly identified and addressed, and established configuration and change management policies can be followed.

Automated and continual compliance testing transforms compliance auditing from a series of fragmented, disconnected, and painful events, to an ongoing, smooth process. A consolidated and continually updated view of compliance data provides an effective and inexpensive way to produce audit reports by eliminating the need for the IT staff to assemble information from multiple, fragmented sources. Consequently, IT organizations can approach upcoming audits more confidently. They will already be well aware of the security situations and know how to address required changes quickly and effectively.

FOSTER COLLABORATION BETWEEN I.T. AND SECURITY

Bridging the gap between an agency's IT operations and security organizations enables the two groups to work closely together to ensure continual compliance. Security teams need ready access to compliance information and reports at all times, not just at audit time. The IT operations staff needs to gather and disseminate this information on an ongoing basis to prevent frequent disruptions.

To meet these requirements, these teams need an automated compliance system that provides detailed, timely compliance information without requiring undue involvement by the IT operations staff. Security teams should be able to see historical trends and reports and easily request new audits when required. However, the security team and IT operations staff should not be allowed to change configurations or force remediation of security issues without following proper configuration and change management processes. The only sure way to achieve this objective is with a single, integrated, and automated platform that performs auditing for compliance and governs the change processes to achieve compliance.

BSM SOLUTION CRITERIA

BSM solutions are available that help federal agency IT organizations meet the challenge of continual compliance. As you evaluate BSM solutions, keep in mind the following important best practices.

IMPLEMENT AND INTEGRATE BEST-PRACTICE PROCESSES

As mentioned previously, many federal IT organizations are adopting ITIL best practices. ITIL provides high-level guidance on what to do but not detailed instructions on how to do it. Consequently, look for BSM solutions that implement — out of the box — processes that are based on ITIL guidelines and that allow you to easily tailor the processes to meet your agency's specific requirements. Such solutions simplify and speed process implementation, resulting in a fast time-to-value.

It's also important to integrate ITIL processes — such as operations, change management, configuration management, and incident and problem management — across IT disciplines. The best way to ensure tight integration is to implement a BSM solution set in which all solutions run on a common platform, one based on a unified and seamless architecture.

BUILD ON A WELL-ARCHITECTED CMDB

A well-architected configuration management database (CMDB) delivers many of the capabilities you need to maintain continual compliance. It provides a single, comprehensive view of the IT environment that allows IT to quickly determine the scope and service impact of any compliance-related issues and to set priorities accordingly. A CMDB also supports the tight integration of processes across solutions by providing a common data source for all BSM solutions. Process integration permits the various IT disciplines to work closely together to maintain compliance. For example, it permits the IT incident and problem management team to collaborate with the change management team to ensure that any changes requested by the former are processed in full compliance with security policies.

Consequently, the BSM solution set should be built on a well-architected CMDB, one that is scalable to accommodate the large IT environments in federal agencies. Look for a CMDB built on a federated architecture to permit access to needed data across the agency without requiring you to move all the data to or replicate it in the CMDB.

The CMDB should also provide an automatic discovery capability for all assets and their physical, logical, and service topologies. Automatic discovery facilitates the initial population of the CMDB, and it keeps the CMDB updated with the latest changes. This ensures that all IT disciplines are working with accurate information.

SUPPORT END-TO-END CHANGE PROCESSES

An effective BSM solution set supports change processes end-to-end — including planning, approval, and implementation — and automatically logs all pertinent change activities. The solution set should continually scan the environment looking for changes. It should provide alerts of unauthorized changes by automatically generating incident tickets whenever it detects changes that have not been implemented according to policy. In addition, it should provide automatic remediation of unauthorized changes wherever possible, such as by removing an unauthorized application from a desktop computer. A BSM solution set that meets these requirements ensures that changes do not violate security policies, so that IT organizations maintain continual compliance.

PROVIDE COMPREHENSIVE, POLICY-BASED AUTOMATION

The BSM solutions should have extensive policy-based automation, encapsulating standards, such as the DISA STIGs, in policies. The solutions should automate routine tasks as well as processes. Process automation needs to encompass the change management, configuration management, and incident and problem management processes.

» Change Management

Automating change management ensures that all changes are made in compliance with established change processes and policies. By automating the change approval process, you ensure that each change is authorized as required. The solution set should provide an audit trail of change processes showing what changes were implemented and when, who implemented them, and who approved them. It needs to notify the people who will be affected by the impending changes and keep those people informed of the change status, including notification when the changes have been successfully completed.

» **Configuration Management**

Look for a BSM solution set that provides automatic provisioning of software and ensures that only compliant configurations are deployed. The solution set should automate the distribution of required software updates and patches, verify their successful distribution and installation, and alert the IT staff to exceptions.

To ensure ongoing compliance with configuration standards, the solution set must be capable of detecting drift from standard configurations caused by unauthorized changes. That requires the ability to automatically test asset configurations against policies and to identify any configurations that are out of compliance. In addition, the solution set should automate remediation wherever possible, such as by removing unauthorized software. It's important to ensure that all remediation changes are implemented according to the change policy by automatically invoking the relevant change management processes.

The solution should also provide configuration automation that reduces the complexity and costs of managing desktops, laptops, and handheld devices. This can be achieved through policy-based automation of application management, inventory, and software usage tracking and software harvesting, as well as advanced PC power settings. By automating these processes, IT departments can proactively and continuously manage the client devices across their enterprise, regardless of their location and connectivity. This dramatically reduces costs, improves quality of service, and reduces the business risk associated with system vulnerabilities. Automating the delivery, installation, updating, repair, removal, and management of applications on desktops, laptops, and mobile devices helps IT departments meet growing service level demands. This also reduces the business risk associated with application downtime and virus attacks.

By tracking software usage for both physical and virtual applications, IT departments can be provided with visibility into which applications are installed across the enterprise, as well as their usage frequency. This knowledge can help IT to minimize potential violation issues, reduce software license purchase costs, and increase the use of existing licenses.

» **Incident and Problem Management**

Moving from a reactive to a proactive mode of managing security-related incidents requires a BSM solution set that immediately alerts the staff to security-related issues. For example, the event management solution should automatically generate an incident ticket when it receives an event that indicates an attempted unauthorized penetration of the IT network. This early warning enables IT to proactively address security issues before they result in the compromise of sensitive information.

THE RESULTS SPEAK FOR THEMSELVES

Implementing BSM solutions to help you achieve and maintain continual compliance with mandated standards and regulations delivers a number of important benefits, including the following:

- » Reduced risk of compromising the security or the availability of information
- » Lower and more predictable compliance costs
- » Greater staff efficiency and less reliance on highly skilled personnel

The benefits of BSM go well beyond compliance. With a BSM solution set that meets the criteria described, you'll improve overall service delivery, with fewer and shorter interruptions to critical business services. In addition, you can achieve higher IT efficiency, lower overall IT costs, and closer alignment of IT to the services your agency provides.

SOME ORGANIZATIONS ARE ALREADY ENJOYING THE ADVANTAGES

Some government IT organizations have implemented BSM solutions to help them meet compliance requirements and are already reaping significant business benefits. Here are some examples:

A major defense agency dramatically reduced the time it takes to perform security-related tasks:

- » Patch 86 Windows systems: Reduced time from 12 – 16 hours to 15 minutes
- » Patch 1 UNIX system: Reduced time from ½ – 2 hours to 5 minutes
- » STIG 1 system: Reduced time from 3 – 5 days to 12 minutes
- » Prove compliance to STIG on 1 UNIX system: Reduced time from 3 – 5 days to 6 minutes
- » STIG 1 virtual machine (VM) system: Reduced time from 5 days to 15 minutes
- » STIG 1 UNIX system: Reduced time from 2 weeks to 15 minutes

Another government agency has an environment that includes 400 Windows servers. The IT organization achieved a cost savings estimated at more than \$500,000 per year through the following time savings:

- » Provision and harden a server: Reduced time from 8 hours to 41 minutes
- » Define policies: Reduced time from 8 hours to 15 minutes
- » Audit and report: Reduced time from 3+ days to 10 minutes
- » Remediate: Reduced time from 5+ days to 1 hour

A leading government systems integrator manages a major portal for a major government agency. The systems integrator owns the infrastructure, applications, and tools, and it performs all ongoing operating system (OS) and application maintenance. The company realized a labor savings in patch management of \$68,500 per year. It reduced standard operating environment (SOE) audit and remediation time by 97 percent, resulting in an estimated labor savings of \$35,496 per year. The systems integrator also eliminated two full-time equivalents (FTEs), resulting in a savings of \$205,000 per year. At the same time, the systems integrator eliminated outages due to misconfigurations. Here are some of the time and labor savings:

- » Patch 112 Windows systems: Reduced time from 40 hours per month to 45 minutes per month
- » Patch 53 UNIX systems: Reduced time from 74 hours per month to 1.3 hours per month
- » SOE audit and remediation: Reduced time from 60 hours per month to 2 hours per month
- » Staff reduction: Reduced staff from 10 FTEs to 8 FTEs

CONCLUSION

The right BSM solution set will enable you to meet the compliance challenge. BSM solutions can help IT organizations transition to a proactive compliance posture and elevate compliance from a periodic auditing exercise to a culture of continual compliance. (An overview of the major frameworks and guides is included in the Appendix section of this white paper).

These solutions can help you define, document, implement, integrate, and automate proven best-practice processes, such as those outlined in the ITIL guidelines, to improve governance and control. You'll provide your IT staff with a single, comprehensive source of information about the IT environment that permits effective and efficient compliance management. In addition, you'll bring the security and IT groups closer together to ensure that security policies are fully understood, properly implemented, and closely monitored for ongoing compliance.

The best part is you'll also position your agency's IT organization to meet the seemingly conflicting mandates most IT organizations — both inside and outside the federal government — face today: improve service while at the same time reducing costs.

BMC offers solutions to help federal government agencies define, implement, integrate, and automate best-practice processes. In fact, in 2009, BMC was awarded the first official ITIL process-compliant certification and trademark. For more information about BMC solutions, visit www.bmc.com/bsm.

END NOTES

1. See the Appendix for an overview of the major frameworks and guides, and of the agencies and organizations responsible for them.
2. <http://nvd.nist.gov/ncp.cfm?repository>

APPENDIX

Table 1 shows the major regulatory frameworks that govern security policy. Table 2 lists the government agencies and other organizations that create, maintain, and distribute security standards and guides. Table 3 lists the implementation guides that are used to implement standards.

Table 1. Security-Related Regulatory Frameworks	
Federal Information Security Management Act of 2002 (FISMA)	<ul style="list-style-type: none"> » Enacted as Title III of the E-Government Act of 2002 » Recognizes the criticality of information security to the economic and national security interests of the United States » Requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by other agencies, contractors, or sources » Defines a framework for managing information security that must be followed for all information systems used or operated by a U.S. federal government agency or by a contractor or other organization on behalf of a federal agency » Defined further by the standards and guidelines developed by the National Institute of Standards and Technology (NIST) as Federal Information Processing Standards (FIPS) publications, and the NIST Special Publications SP-800-series
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	<ul style="list-style-type: none"> » Amends the internal revenue code of 1996 to improve the portability and continuity of health insurance coverage in the group and individual markets; to combat waste, fraud, and abuse in health insurance and health care delivery; to promote the use of medical savings accounts; to improve access to long-term care services and coverage; to simplify the administration of health insurance; and to serve other purposes » Impacts IT organizations through requirements laid out in NIST publication SP 800-66, which primarily concerns safeguarding health information on IT systems

Table 2. Major Standards Organizations	
National Institute of Standards and Technology (NIST)	<ul style="list-style-type: none"> » The Cyber Security Research and Development Act requires NIST to develop, and revise as necessary, a checklist of settings and options that minimize the security risks associated with each computer hardware or software system that is currently, or is likely to become, widely used within the federal government » Maintains — through the NIST Computer Security Division, the Special Publication 800 series documents — a set of documents that report on NIST Information Technology Laboratory (ITL) research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations » Provides recommended security controls for federal information systems through SP 800-53, developed under the Federal Information Security Management Act of 2002 (FISMA); provides recommended security controls for federal information systems.
Defense Information Systems Agency (DISA)	<ul style="list-style-type: none"> » Develops and distributes security configuration guides for a wide variety of software and documents them in Security Technical Implementation Guides (STIGs)
National Security Agency/Central Security Service (NSA/CSS)	<ul style="list-style-type: none"> » Responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves a significant amount of cryptography » Develops and distributes security configuration guides for a wide variety of open source and proprietary software » Has recently been directed to help monitor U.S. federal agency computer networks to protect them against attacks
Center for Internet Security (CIS)	<ul style="list-style-type: none"> » A not-for-profit organization that helps enterprises reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls, and provides enterprises with resources for measuring information security status and making rational security investment decisions

Table 3. Security Implementation Guides

<p>Security Technical Implementation Guide (STIG)</p>	<ul style="list-style-type: none"> » A methodology for standardized, secure installation and maintenance of computer software and hardware » Used to maintain the confidentiality, integrity, and availability of an information system and is an important part of configuration management for the system » Contains implementation guidelines that include recommended administrative processes that span the lifecycle of the device » Can be used, for example, to specify the configuration of desktop computers to minimize susceptibility to network-based attacks and also to prevent system access by a computer criminal who is within reach of the device » May also be used to describe the processes and lifecycles for maintenance (such as software updates and vulnerability patching)
<p>Federal Desktop Core Configuration (FDCC)</p>	<ul style="list-style-type: none"> » An Office of Management and Budget (OMB)-mandated security configuration » Currently exists for Microsoft Windows Vista and XP operating system software » Originally called for in a March 22, 2007, memorandum from OMB to all federal agencies and department heads and in a corresponding memorandum from OMB to all federal agency and department chief information officers (CIO), although not addressed specifically as the "Federal Desktop Core Configuration"

Business runs on IT. IT 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.

About the Authors

Chris Olson is the technical director and CTO for Public Sector Sales at BMC Software. Olson manages the day-to-day technical sales engineering activities for all federal, state and local, and education accounts. Olson explores issues related to the federal sector and how BSM addresses compliance and other requirements. He is also Service Manager-certified in ITIL. Previously, he worked as a sales engineer, supporting various government and commercial accounts at BMC and Symantec Corporation. He began his career in IT and computer science in the U.S. Air Force. After leaving the Air Force, he worked in various positions developing software for Department of Defense-related programs.

Ben Newton is the technical director for Department of Defense and Intelligence Community Sales at BMC Software. Newton manages the technical side of the sales cycle for all of BMC's defense and intelligence community customers. He came to BMC with the acquisition of BladeLogic, Inc., where he was a senior application engineer. For the last nine years, he has specialized in the various aspects of data center automation, particularly application release and compliance automation. Before BladeLogic, he worked as a systems architect for EDS and Northrop Grumman, where he was the lead architect for the design of the Army Knowledge Online (AKO) Disaster Recovery project. He graduated in 2000 from Cornell University with a master's degree in computer science.

To learn more about how BMC can help activate your business, visit www.bmc.com or call (800) 841-2031.

