



BMC Software Solutions for the Payment Card Industry

PCI DSS Compliance – Protecting Cardholder Data is the Core Goal and Purpose

The Payment Card Industry (PCI) Data Security Standard (DSS) encourages cardholder data security and facilitates the broad adoption of consistent data security measures globally. Consumers, trading partners, regulators, legislators and shareholders demand that any organization which accepts or processes credit card payments comply with the PCI DSS. Companies that fail to protect consumer data stand to lose millions of dollars in fines, lost sales, reduced shareholder value and squandered customer confidence.

To ensure adherence, credit card companies have offered incentives for organizations that comply. For example, Visa USA has announced \$20 million in financial incentives for larger banks that process more than 1 million transactions per year and can ensure their transactions are PCI compliant.

The PCI DSS is comprised of six major groups that contain twelve major requirements, which refer to over 210 specific requirements. The sheer volume of individual specific requirements suggests a stepwise and phased approach based upon risk weighting and value prioritization, based on a company's unique parameters. It is important to "do the right thing the right way."

AUTOMATION, PCI DSS AND COMPLIANCE

BMC Software offers you a better approach to managing PCI DSS compliance. As the recognized leader in Business Service Management (BSM), BMC is uniquely positioned to help you succeed in your compliance efforts by providing a comprehensive and modular approach that can unify, automate and enforce policies and governance models across your entire IT organization.

BSM solutions from BMC help organizations become PCI DSS compliant by managing the identity and authorization of entities or people that access data related to cardholder data and protecting that data. The solutions address PCI DSS standards by supporting and automating the processes identified in the over 210 requirement specifications identified in the twelve major requirements under the six major categories.

The BMC solution helps you:

- » Define and manage controls designed to meet objectives and mitigate risks across all the critical functions of IT.
- » Manage and control user access to critical applications and automate access certifications based on user roles and organizational policies.
- » Manage, automate and control the change lifecycle to ensure that PC, network and server configurations remain compliant — from planning and approval through execution and verification.
- » Adopt and automate IT best practices.

With a platform-based approach, the output of one function becomes the input to another. For example, the output of request management is an input to change management. This integration, with an audit trail and evidence, will improve the "audit posture" and can result in improved audit results.

BSM solutions from BMC address the wide range of controls that help organizations comply with PCI DSS requirements, as described in the following sections.

BUILD AND MAINTAIN A SECURE NETWORK

Requirement

Install and maintain a firewall configuration to protect cardholder data

How BSM from BMC Addresses this Requirement

- » Provides ITIL certified change management and problem management processes for managing and tracking change activity in systems containing cardholder data.
- » Performs automated audits for “configuration drift” detection across servers, clients, and networks that contain cardholder data

Requirement

Do not use vendor-supplied defaults for system passwords and other security parameters

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to policies and procedures for ensuring proper disposition of vendor-supplied defaults for system passwords and other security parameters.
- » Automated account creation, including password randomization, and requiring that passwords be changed when a user first logs in.

PROTECT CARDHOLDER DATA

Requirement

Protect stored cardholder data

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to policies and procedures for identifying legal, regulatory, and business requirements for data retention, including specific retention of cardholder data.
- » Provides the framework to manage attestations to policies and procedures for the security and proper disposal of cardholder data
- » Provides the framework to manage attestation to policies and procedures for quarterly review of disposal procedures and results to ensure cardholder data has been disposed of according to retention period policies.

Requirement

Encrypt transmission of cardholder data across open, public networks

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to review evidence of the presence of and successful use of mechanisms to encrypt data being transmitted, and mechanisms to ensure that data in flight is not improperly modified.
- » Performs configuration audits and assessments to ensure mechanisms for encrypting and decrypting cardholder data remain configured, installed and enabled.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement

Use and regularly update anti-virus software on all systems commonly affected by malware

How BSM from BMC Addresses this Requirement

- » Package and deploy anti-virus software
- » Detect and remediate clients and servers whose antivirus protection is not current
- » Generate reports on which clients and servers are out of compliance with antivirus policies.
- » Provides ITIL certified change management and problem management processes for managing and tracking change activity in systems containing card-holder data.

Requirement

Develop and maintain secure systems and applications

How BSM from BMC Addresses this Requirement

- » Scans all of an organization's systems for a vendor-supplied or custom list of patches, automatically download, deploy and verify the deployment of the patches, and generate reports on adherence to patch policies.
- » Provides ITIL certified change management and problem management processes for managing and tracking change activity in systems containing card-holder data.
- » Has the platform for reporting suspected or known security incidents and to instantiate and track containment, remediation, and response activities

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement

Restrict access to cardholder data by business need-to-know

How BSM from BMC Addresses this Requirement

- » Provides role-based access control (RBAC) and identity management provisioning.
- » Leverages ITIL certified change management processes for protection and enforcement of identities.
- » Includes key identity risk factors for users defined.

Requirement

Assign a unique ID to each person with computer access

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to security reminders and corporate guidelines that address unique identity policy.
- » Ensures that unique names and numbers are assigned, provisioned, and tracked for user identities.
- » Leverages ITIL certified change management processes for protection and enforcement of IOs and identities.

Requirement

Restrict physical access to cardholder data

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to the plan for contingency operations access processes, the facility security plan, and facility maintenance record keeping processes.
- » Leverages the service desk and change management for repairs and modifications to the physical security components of a facility.
- » Provides input to the control and validation of access to facilities based on role or function, including visitor control.

REGULARLY MONITOR AND TEST NETWORKS

Requirement

Track and monitor all access to network resources and cardholder data

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to the review of records, server logs, and monitor logs that contain activity in the information systems using cardholder data.
- » Generates comprehensive reports of system access by individual users.
- » Provides audit trail of specific changes made by individual users.
- » Provides tracking and audit trail for attempts to access data, change systems configurations, create or delete system level objects, view audit trails, or log in by individual users, including systems administrators.

Requirement

Regularly test security systems and processes

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to regular (at least quarterly) testing for wireless access points and regular internal and external vulnerability scans.
- » Provides the framework to manage attestations to regular (at least annually) internal and external penetration testing.
- » Performs configuration audits and assessments to ensure that FIM, intrusion detection, and/or intrusion prevention systems remain configured, installed and enabled.

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement

Maintain a policy that addresses information security

How BSM from BMC Addresses this Requirement

- » Provides the framework to manage attestations to security reminders, security procedures, and guidelines for PCI DSS.
- » Provides the framework to manage attestations to an annual process that identifies threats and vulnerabilities and results in a formal risk assessment
- » Provides the framework to manage attestations to the development and use of daily operational security procedures that are consistent with the PCI DSS specifications.

**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 provides a comprehensive and unified platform that helps IT organizations cut cost, reduce risk and drive business profit. For the four fiscal quarters ended March 31, 2010, BMC revenue was approximately \$1.91 billion.



BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. ITIL® is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office, and is used here by BMC Software, Inc., under license from and with the permission of OGC. All other trademarks or registered trademarks are the property of their respective owners. © 2010 BMC Software, Inc. All rights reserved.

