Security information and event management solutions
To support your IT objectives

Tivoli® software

Address the PCI Data Security Standard with IBM Tivoli Security Information and Event Manager.

Highlights

- Develop a comprehensive, heterogeneous security monitoring solution to address PCI DSS and other security management issues
- Facilitate compliance management efforts with centralized log management, dashboard and reporting capabilities
- Help protect proprietary customer information by auditing the behavior of all users — privileged and unprivileged
- Manage security operations effectively and efficiently with centralized security event correlation, prioritization, investigation and response
- Support operating system, database and application auditing

Review PCI requirements

Today, more than one billion people worldwide use a variety of payment cards to support commercial transactions in almost every business around the world.* The use of these payment cards represents an enormous opportunity for businesses to increase sales through channels such as online shopping.

However, the information associated with these payment cards — commonly referred to as “cardholder data” — is the focus of a growing number of identity theft activities.

To address the need to improve payment card security, the card industry has created a set of global requirements called the Payment Card Industry (PCI) Data Security Standard (DSS). Essentially, PCI DSS is a set of 12 data-centric control objectives and associated requirements for helping to ensure the security and privacy of cardholder data.

Support and automate compliance management efforts

Addressing PCI DSS can demand significant and broad-based commitments in terms of people, time and technology resources. To support this commitment, IBM Tivoli® Security Information and Event Manager provides a comprehensive solution designed to effectively monitor, audit and report on user activity and security events across the enterprise.

Often, attempts to develop security information and event management (SIEM) solutions usually involve one vendor providing an organization with an intrusion and incident management

PCI Data Security Standard	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

The PCI DSS includes 12 requirements — referred to as the "digital dozen" — that organizations must meet each year to maintain PCI compliance.

dashboard — while another vendor provides the dashboard to assess how well the organization adheres to its governance policies. The result can be poor visibility due to weak product integration, compliance management gaps, or expensive and time-consuming customization.

With Tivoli Security Information and Event Manager, today's organizations now have a fully integrated, broad-based SIEM solution to help support and automate compliance efforts involving all 12 PCI standards. Combining real-time monitoring with in-depth historical analysis and reporting, Tivoli Security Information and Event Manager is able to:

- Collect and centralize PCI DSS–relevant security log data from heterogeneous sources.
- Filter collected information against PCI requirements and corporate security policy.
- Automatically trigger appropriate alerts upon detecting suspicious activities regarding payment card security.
- Archive PCI DSS–relevant log data for review.
- Provide consolidated viewing and reporting through a centralized dashboard.

Tivoli Security Information and Event Manager provides organizations with its unique W7 methodology, designed to rapidly determine the seven critical W's of security: Who, did What, When, Where, Where from, Where to and on What. By revealing who touched what information asset and comparing that activity to policies defining appropriate use, organizations can automate monitoring requirements and help accelerate their compliance management efforts for PCI.

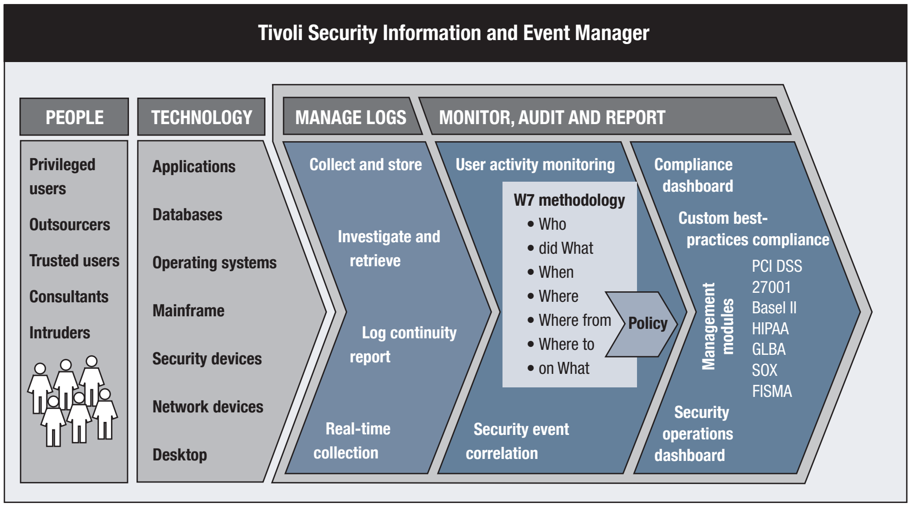
For mainframe environments, the IBM Tivoli zSecure suite provides administrative and audit capabilities for IBM Resource Access Control Facility (RACF®), CA ACF2™ and CA Top Secret®. The suite works directly with Tivoli Security Information and Event Manager to create an enterprise-wide security audit and compliance architecture. As a critical part of the zSecure suite, IBM Tivoli zSecure Audit provides reporting on PCI-relevant policy settings and exceptions at user-specified timeframes.

Tivoli zSecure Audit alerts can be easily configured to help ensure that high-priority policy exceptions are handled immediately. Tivoli zSecure Audit also offers the capability to fingerprint sequential log data residing on both tape and direct access storage device (DASD) media. This enables periodic reviews to check the integrity of System Management Facility (SMF) logs on tape and DASD.

Enhance compliance management efforts

Tivoli Security Information and Event Manager collects logs from a wide array of device types and offers an "at-a-glance" log continuity report that helps demonstrate to auditors that each and every log is collected as required. It includes a robust enterprise audit dashboard that links day-to-day operational data to the policy-based analysis required for auditing. The user activity monitoring capabilities enable chief information security officers (CISOs) and auditors to receive a consolidated view of all relevant activities in the enterprise, including how much activity has been logged and how users' profiles compare with the information they are accessing.

Tivoli Security Information and Event Manager provides a number of management modules, including one for PCI DSS. Each module provides detailed information and templates to use when managing PCI compliance initiatives. Each module includes an asset classification template, a policy template to measure event data against custom policies and a report center that provides reports geared to PCI requirements.



Tivoli Security Information and Event Manager provides a critical dashboard from which to view the organization's security posture. It also includes a PCI DSS management module and PCI-specific reports, facilitating the link between the security posture and the compliance posture.

In addition, Tivoli Security Information and Event Manager provides a robust, unified platform from which to automate incident recognition and response, streamline incident handling, and enable policy monitoring and enforcement. As a result, organizations can implement a proven, automated security event aggregation and correlation methodology to help optimize resources, reduce the complexity of managing security, enforce security policy and help improve their overall security posture.

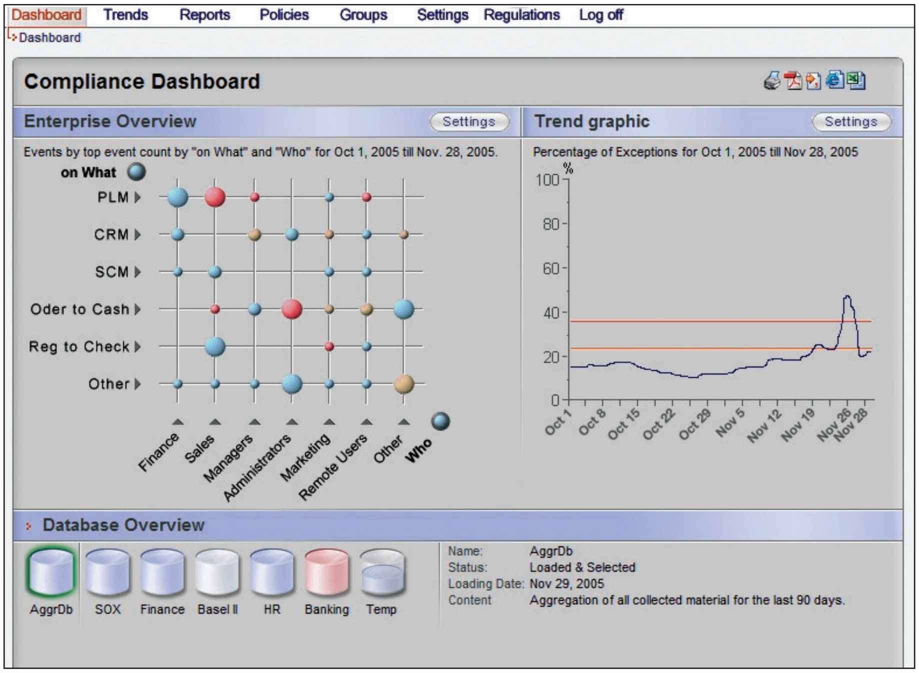
Continuous compliance management

No single tool is a complete solution for meeting all of the requirements of PCI DSS or compliance with any data protection or privacy initiative. Furthermore, compliance activities are a moving target. Even after gaps have been filled and the organization has successfully passed an assessment, continued monitoring is needed to support ongoing compliance initiatives. To support this need, Tivoli Security Information and Event Manager provides a systematic approach to dependable monitoring while helping to reduce preparation and reporting costs for PCI and other initiatives.

Tivoli Security Information and Event Manager can also be used for cross-compliance management efforts — an important capability today since organizations can be subject to multiple requirements.

Explore end-to-end Tivoli security solutions

In addition, other IBM solutions are available to help support PCI DSS requirements. For identity management, IBM Tivoli Identity Manager provides a secure, automated and policy-based solution designed to manage user privileges across heterogeneous IT resources. The IBM Tivoli Access Manager family of products helps organizations securely manage access to business-critical applications and data while giving users fast, convenient access to the information they need.



Compliance Dashboard

Enterprise Overview

Events by top event count by "on What" and "Who" for Oct 1, 2005 till Nov. 28, 2005.

Trend graphic

Percentage of Exceptions for Oct 1, 2005 till Nov 28, 2005

Database Overview

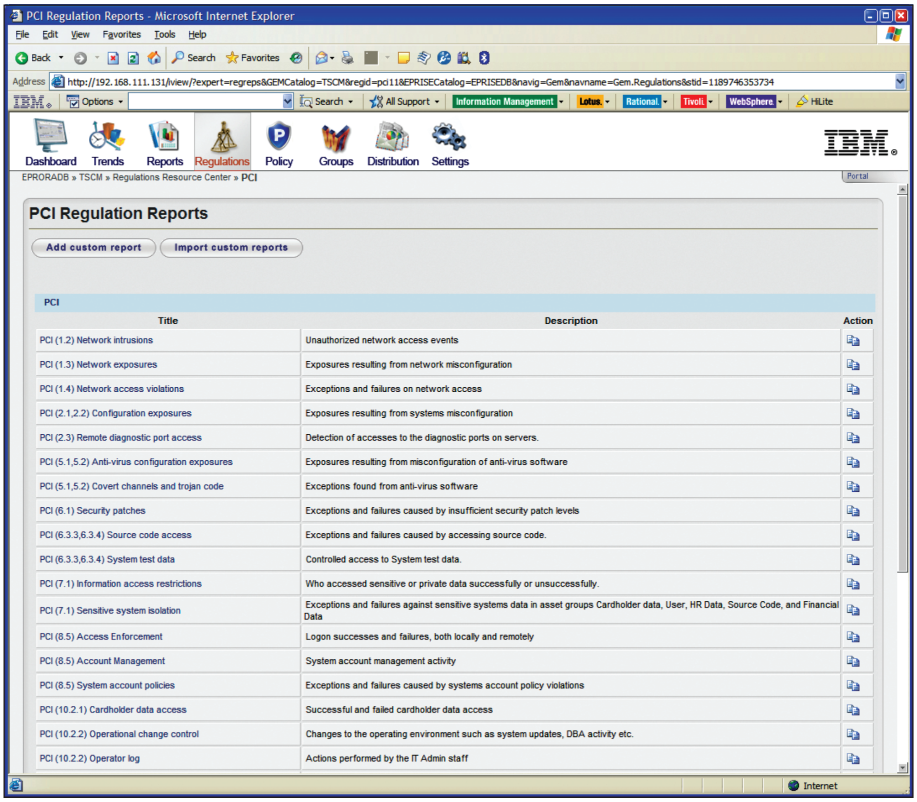
Name: AggrDb
Status: Loaded & Selected
Loading Date: Nov 29, 2005
Content Aggregation of all collected material for the last 90 days.

With Tivoli Security Information and Event Manager, users can view all activities in the enterprise from one enterprise audit dashboard. The size of each circle above indicates the amount of activity (logged events). Across the axes, we see a comparison of people (Who) with information (on What).

IBM Managed Firewall Service can be used for outsourcing all firewall services, including the firewall management requirements needed to ensure compliance with PCI. For companies that want to manage their own firewalls, IBM Tivoli Application Dependency Discovery Manager can help create a “network map” of the IT components — including the location of firewalls — as specified by PCI requirements.

IBM Tivoli Change and Configuration Management Database (CCMDB) can be applied to standardize the processes for making changes to firewalls. IBM Tivoli Security Compliance Manager can be used to monitor firewall configuration files, ensuring that they have not been modified outside of the standardized processes.

Organizations can also take advantage of IBM expertise and experience in IT



Address: http://192.168.111.131/iview/?expert=regreps&GEMCatalog=TSCM&regid=pci11&EPRISECatalog=EPRISEDB&navig=Gem&navname=Gem.Regulations&stid=1189746353734

EPRORADB » TSCM » Regulations Resource Center » PCI

PCI Regulation Reports

PCI

Title	Description	Action
PCI (1.2) Network intrusions	Unauthorized network access events	⧉
PCI (1.3) Network exposures	Exposures resulting from network misconfiguration	⧉
PCI (1.4) Network access violations	Exceptions and failures on network access	⧉
PCI (2.1,2.2) Configuration exposures	Exposures resulting from systems misconfiguration	⧉
PCI (2.3) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.	⧉
PCI (5.1,5.2) Anti-virus configuration exposures	Exposures resulting from misconfiguration of anti-virus software	⧉
PCI (5.1,5.2) Covert channels and trojan code	Exceptions found from anti-virus software	⧉
PCI (6.1) Security patches	Exceptions and failures caused by insufficient security patch levels	⧉
PCI (6.3.3,6.3.4) Source code access	Exceptions and failures caused by accessing source code.	⧉
PCI (6.3.3,6.3.4) System test data	Controlled access to System test data.	⧉
PCI (7.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.	⧉
PCI (7.1) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups Cardholder data, User, HR Data, Source Code, and Financial Data	⧉
PCI (8.5) Access Enforcement	Logon successes and failures, both locally and remotely	⧉
PCI (8.5) Account Management	System account management activity	⧉
PCI (8.5) System account policies	Exceptions and failures caused by systems account policy violations	⧉
PCI (10.2.1) Cardholder data access	Successful and failed cardholder data access	⧉
PCI (10.2.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.	⧉
PCI (10.2.2) Operator log	Actions performed by the IT Admin staff	⧉

Tivoli Security Information and Event Manager provides more than 30 report templates specific to helping manage PCI compliance efforts.

implementations, business process development and general consulting. IBM has a global presence with more than 3,500 security and privacy experts worldwide. We have experience in virtually every industry, with consultants who understand the unique business problems and requirements of each industry.

Summary

Tivoli Security Information and Event Manager has helped numerous organizations with their PCI DSS compliance management initiatives, providing solutions designed to enable policy monitoring and enforcement; establish an audit trail; receive alerts and generate compliance reports; archive crucial security log information; and conduct investigations when a PCI-relevant concern arises.

By taking full advantage of Tivoli Security Information and Event Manager and other IBM offerings, organizations can develop integrated, end-to-end processes that encompass all aspects of security planning, management and reporting designed to support PCI requirements and other mandates.

For more information

To learn more about how Tivoli Security Information and Event Manager and related offerings from IBM help you address PCI requirements, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

About IBM Tivoli service management software

Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation — visibility to see and understand the workings of their business; control to effectively manage their business, minimize risk and protect their brand; and automation to optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization's most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients and Business Partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
June 2008
All Rights Reserved

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

*PCI Security Standards Council

TAKE BACK CONTROL WITH Tivoli.