MAPPING PCI DSS WITH 8MAN

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. PCI applies to all organisations or merchants, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.

8MAN, an intuitive access rights management solution, builds a robust security process that supports a variety of regulatory needs of enterprises. It limits access rights to a 'need to know' basis, thereby significantly mitigating data security risks. Organisations using fileservers, Active Directory, Exchange and SharePoint can easily view, manage, provision and delegate access rights with the help of 8MAN.

The following checklist provides a quick overview of how 8MAN supports PCI DSS requirements such as restricting access to cardholder data on a business need to know basis, assigning a unique ID to each person with computer access, tracking and monitoring all access to network resources and cardholder data and maintaining a policy that addresses information security.

About us:

protected-networks.com was founded in Berlin in 2009 and develops 8MAN, an integrated software solution for access rights management in Windows and in VMware vSphere™ environments.

www.8man.com

Germany (Head office)

protected-networks.com GmbH

Alt-Moabit 73
10555 Berlin

Tel. +49 (0) 30 390 63 45 - 0
Fax +49 (0) 30 390 63 45 - 51

info@protected-networks.com
www.protected-networks.com

UK

protected-networks.com

1 Stanhope Gate
Camberley, Surrey , GU15 3DW

+44 (0) 1276 919 989
uk@8man.com

8MAN
PCI DSS

MAPPING PCI DSS WITH 8MAN

Requirements	Section Detail	8MAN
Requirement 7: Restrict access to cardholder data by business need to know.	**7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	
	7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** 8MAN Access Reports check which user has what access rights. All modifications to access rights are logged along with a corresponding comment, explaining why the permissions were altered.
	7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Default templates and give users access to only those groups which are necessary for their role.
	7.1.3 Requirement for a documented approval by authorised parties specifying required privileges.	**7.1.3** In 8MAN it is mandatory to enter a comment for each change. You can also add links to documents.
Requirement 8: Assign a unique ID to each person with computer access.	**8.5** Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	
	8.5.4 Immediately revoke access for any terminated users.	**8.5.4** With 8MAN, terminated users can be soft-deleted, i.e. deactivated and moved to a separate OU, to ensure access termination.
Requirement 10: Track and monitor all access to network resources and cardholder data.	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:	
	10.2.1 Verify all individual access to cardholder data is logged.	**10.2.1** 8MAN File Server (FS) Logga audit functionalities meet this requirement.
	10.2.2 Verify actions taken by any individual with root or administrative privileges are logged.	**10.2.2** 8MAN FS Logga audit functionalities meet this requirement.
Requirement 12: Maintain a policy that addresses information security for all personnel.	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:	
	12.5.4 Verify that responsibility for administering user account and authentication management is formally assigned.	**12.5.4** 8MAN can create, administer, change and soft delete user accounts.
	12.5.5 Verify that responsibility for monitoring and controlling all access to data is formally assigned.	**12.5.5** 8MAN FS Logga audit functionalities meet this requirement.

NEXT STEPS

Meeting PCI DSS requirements with 8MAN enables companies to achieve both IT compliance and best practice. To find out how 8MAN can help your organisation operate in a secure environment, contact us to arrange an interactive online demonstration.