



Cisco MARS Blog

A technological journey into the myths and wonders of the Cisco MARS appliance.

CS-MARS Compliance to Canned Report Mapping

Managing Risk and Compliance with CS-MARS is a straight forward process with over 100 built in reports covering many forms of regulatory compliance. Reporting with CS-MARS focuses on aligning information security systems, applications, and networks data with the requirements of compliance guidelines specific to your organization.

The Cisco Self-Defending Network (SDN) is the first line of corporate defense because it is the foundation for all of an organization's data, applications, and business processes. The Cisco SDN provides an end-to-end system-based approach to network security that supports industry control frameworks and best practices. This approach helps organizations better manage network security while preparing them to meet regulatory compliance requirements.

Each organization should carefully consider the appropriate network security control objectives for its own circumstances, size, and complexity. CS-MARS reports should not be the complete basis for audit reliance. Cisco suggests that organizations discuss IT control approaches with their external auditors to gain perspective on IT control objectives and specific compliance reports that are required."

The CS-MARS interface allows organizations to modify the canned reports to meet their specific needs in addition to providing organizations a starting framework for building reports based upon their audit requirements. Additionally, CS-MARS has an easy to use reporting interface which allows organizations to build custom reports specifically aligned to their networks and the audit requirements they must adhere to.

The report to compliance mappings contained in this document are guidelines and should not be considered to be the complete list of reports needed to meet each form of compliance or legislative requirements.

Compliance and Risk Management: SOX



http://www.cisco.com/en/US/netsol/ns625/net_value_proposition0900aecd80380886.html

COBIT Control Objective	COBIT Objective Requirement	Related CS-MARS Reports
COBIT- DS 3.3 : Monitoring and reporting	Ensure that performance of IT resources is continuously monitored and exceptions are reported in a timely and comprehensive manner	Resource Issues: Network - Top Reporting Devices Resource Issues: Server - Top Reporting Devices Resource Utilization: Bandwidth: Inbound - Top Interfaces Resource Utilization: Bandwidth: Outbound - Top Interfaces Resource Utilization: CPU - Top Devices Resource Utilization: Concurrent Connections - Top Devices Resource Utilization: Errors: Inbound - Top Interfaces Resource Utilization: Errors: Outbound - Top Interfaces Resource Utilization: Memory - Top Devices Operational Issues: Network - Top Reporting Devices Operational Issues: Server - Top Reporting Devices Operational Issues: Network - All Events Operational Issues: Server - All Events
COBIT - DS 5.2: Identification, Authentication and Access	Ensure that logical access to and the use of IT resources are restricted by the implementation of adequate identification, authentication and authorization mechanisms linking users and resources with access rules	Activity: Host Login Success - All Events Activity: Host Privilege Escalation - All Events

		<p>Activity: Host Admin Login Success - All Events</p> <p>Activity: Network Device Login Success - All Events</p> <p>Activity: Remote Access Login - All Events</p>
COBIT-DS 5.4: Management review of user accounts	Management should have a control process to review and confirm access rights	<p>Activity: Host User/Group Management - All Events</p> <p>Activity: Host User/Group Management - Top hosts</p> <p>Activity: Database User/Group Change Successes - All Events</p> <p>Activity: Database User/Group Change Successes - Top Users</p>
COBIT - DS 5.7: Security Surveillance	Ensure that security activity is logged and any implication is reported immediately	<p>Activity: All - Top Reporting Device Types</p> <p>Activity: All - Top Reporting Devices</p> <p>Activity: Attacks Seen - Top Reporting Devices</p>
COBIT - DS 5.10: Violation and Security Activity Reports	Ensure that violation and security activity is logged, reported, reviewed and appropriately escalated	<p>Activity: Host Login Failures - All Events</p> <p>Activity: Host Login Failures - Top Destinations</p> <p>Activity: Host Login Failures - Top Users</p> <p>Attacks: Password - Top Destinations</p> <p>Attacks: Password - All Events</p> <p>Attacks: Privilege Escalation Failures - All Events</p> <p>Activity: Database Privileged Command Failures - All Events</p> <p>Activity: Database Privileged Command Failures - Top Users</p> <p>Activity: Database Regular Command Failures - All Events</p> <p>Activity: Database Regular Command Failures - Top Users</p> <p>Activity: Database User/Group Change Failures - All Events</p> <p>Activity: Database User/Group Change Failures - Top Users</p>

		<ul style="list-style-type: none"> Attacks: All - Top Destinations Attacks: All - Top Event Types Attacks: All - Top Event Type Groups Attacks: All - Top Rules Fired Attacks: All - Top Sources Attacks: SANS Top 20 - Top Event Types Attacks: Database Server - Top Event Types Attacks: Web Server/App - Top Event Types Attacks: Login Services - Top Event Types Attacks: Mail Server - Top Event Types Attacks: RPC Services - Top Event Types Attacks: FTP Server - Top Event Types Activity: IDS Evasion - Top Event Types Attacks: Identity Spoofing - Top Event Types Attacks: Network DoS - Top Event Types Activity: Stealth Scans - Top Sources Activity: Scans - Top Destinations Activity: Scans - Top Destination Ports
COBIT - DS 5.19: Malicious software prevention, detection and correction	<p>establish a framework of adequate preventative, detective and corrective control measures for malicious software such as computer viruses and trojan horses...</p>	<ul style="list-style-type: none"> Attacks: Virus/Worms - Top Sources Activity: Virus/Worms - Top Event Types Activity: Virus/Worms - Top Infected Hosts Activity: Virus: Detected - Top Users Activity: Virus: Infections - Top Users Activity: Security Posture Not Up To Date - All Events Activity: Security Posture Not Up To Date - Top Users Activity: Security Posture Up To Date - Top Users Activity: Security Posture Validation Failure - Top Users

		Activity: Security Posture w/o Credentials - Top Hosts Activity: Spyware - Top Hosts
COBIT - DS 5.20: Firewall architectures and connections with public networks	Adequate firewalls should be operative to protect against DoS and any unauthorised access to internal resources	Activity: Network Usage - Top Destination Ports Activity: Network Usage Inbound - Top Ports Activity: Network Usage Inbound - Top Destinations Activity: Network Usage Outbound - Top Ports Activity: Network Usage Outbound - Top Destinations Activity: Denies Inbound - Top Destination Ports Activity: Denies Inbound - Top Destinations Activity: Denies Inbound - Top Sources Activity: Denies Outbound - Top Destination Ports Activity: Denies Outbound - Top Destinations Activity: Denies Outbound - Top Sources Activity: Attacks Prevented - Top Reporting Devices Resource Utilization: Concurrent Connections - Top Devices
COBIT - DS 9.4: Configuraton Control	Ensure that the existence and consistency of IT configuration is periodically checked	Configuration Changes: Network - All Events Activity: Database Object Modification Successes - All Events Activity: Host Registry Changes - All Events Activity: Host Security Policy Changes - All Events
COBIT - DS 9.5: Unauthorized software	Business and IT management should periodically check the organization for unauthorized software	Activity: P2P Filesharing/Chat - Top Event Types Activity: P2P Filesharing/Chat - Top Hosts Activity: Recreational - Top Sources

Activity: Spyware - Top Hosts

Attacks: Uncommon or Anomalous Traffic - Top Event Types

Activity: IRC Activity - Top Hosts

Activity: Covert Tunnels - Top Hosts

Cisco Self-Defending Network Support for PCI Data Security Standard



http://www.cisco.com/application/pdf/en/us/guest/netso/ns625/c714/cdecont_0900aecd80500533.pdf

PCI Objective	PCI Requirements	Related CS-MARS Reports & Tools
Maintain a Secure Network	1 - Incident & Case Detail	Attack: All - Top Rules Fired Incident TAB - GUI - Choose time period Case Management TAB - Case Details All Matching Sessions - Any Confirmed Positive Firing Event Network Status Page - Top Rules Fired Activity: All Incident Reports - Network Related <i>Customer Report based upon Customer Created Rules</i> Summary > Network Status Tab > Incidents Graph Summary > Network Status Tab > Top Rules Fired Graph Summary > Network Status Tab > Top Event Types Graph
	1 - Violation by Rule	Attacks: All - Top Event Types Attacks: All - Top Event Type Groups Attacks: All - Top Rules Fired <i>Can customize for just Valid Networks, leaving out hosts.</i>
	1 - Summary of Incidents	Summary > Dashboard Incidents > Filter on Rules - Network related <i>Rules Fired = Incidents in MARS</i> Summary > Network Status > Incidents Graphs Summary > Network Status > Top Rules Fired Graph/Report

Activity: Attacks Seen - Top Reporting Devices
Attacks: All - Top Rules Fired - *can filter on networks only*

**Protect
cardholder Data -
Database Servers
& File Servers**

3 - Incident and
Case Detail

Attack: All - Top Rules Fired
Incident TAB - GUI - Choose time period
Case Management TAB - Case Details
Activity: **All Incident Reports - Server Related**
Customer Report based upon Customer Created Rules

3- Violation by Rule

Activity: Host Login Success - All Events Filter for Db servers
Activity: Host Privilege Escalation - All Events Filter for Db servers
Activity: Host Admin Login Success - All Events Filter for Db servers
Activity: Database User/Group Change Successes - All Events
Activity: Database User/Group Change Successes - Top Users
Activity: Host Login Failures - All Events
Activity: Host Login Failures - Top Destinations
Activity: Host Login Failures - Top Users
Activity: Database Privileged Command Failures - All Events
Activity: Database Privileged Command Failures - Top Users
Activity: Database Regular Command Failures - All Events
Activity: Database Regular Command Failures - Top Users
Activity: Database User/Group Change Failures - All Events
Activity: Database User/Group Change Failures - Top Users
Attacks: Database Server - Top Event Types
Activity: Database Object Modification Successes - All Events
Activity: Host Registry Changes - All Events
Activity: Host Security Policy Changes - All Events
Operational Issues: Server - Top Reporting Devices

Operational Issues: Server - All Events

Maintain a Vulnerability Management Program

4 - Asset Detail

Activity: Host User/Group Management - All Events
Activity: Host User/Group Management - Top hosts
Activity: Host Registry Changes - All Events
Activity: Host Security Policy Changes - All Events

Custom Report - All Matching Events - CS-MARS imported Vulnerable host from VA scanner

Custom Report - All Matching Events - CS-MARS updated Vulnerable host from VA scanner

Custom Report - All Matching Events - CS-MARS deleted Vulnerable host via VA scanner input
Management > IP Management > *choose host*

PCI Requirement

10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is difficult without system activity logs.

Sub-requirements:

10.1 Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.

10.2 Implement automated audit trails to reconstruct the following events, for all system components:

10.2.1 All individual user accesses to cardholder data

10.2.2 All actions taken by any individual with root or administrative privileges

10.2.3 Access to all audit trails

10.2.4 Invalid logical access attempts

10.2.5 Use of identification and authentication mechanisms

10.2.6 Initialization of the audit logs

10.2.7 Creation and deletion of system-level objects

10.3 Record at least the following audit trail entries for each event, for all system components:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource

10.4 Synchronize all critical system clocks and times.

10.5 Secure audit trails so they cannot be altered:

10.5.1 Limit viewing of audit trails to those with a job-related need.

10.5.2 Protect audit trail files from unauthorized modifications.

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.

10.5.5 Use file integrity monitoring and change detection software (such as Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

10.6 Review logs for all system components at least daily. Log reviews should include servers that perform security functions like IDS and authentication (AAA) servers (RADIUS, for example).

10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations. An audit history usually covers a period of at least one year, with a minimum of three months available online.

PCI Requirement

11: Regularly test security systems and processes.

Vulnerabilities are continually being discovered by hackers and researchers, and introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and through changes.

Sub-requirements:

11.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts. Where wireless technology is deployed, use a wireless analyzer periodically to identify all wireless devices in use.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (new system component installations, changes in network topology, firewall rule modifications, or product upgrades, for example).

Note: External vulnerability scans must be performed by a scan vendor qualified by the PCI.

11.3 Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (operating system upgrade, subnetwork added to environment, Web server added to environment, for example).

11.4 Use network IDSs, host-based IDSs and IPSs to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.

11.5 Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files, and perform critical file comparisons at least daily (or more frequently if the process can be automated). Critical files do not necessarily contain cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the merchant or service provider.

Compliance and Risk Management: GLBA

http://www.cisco.com/en/US/netsol/ns625/net_value_proposition0900aecd80380856.html



GLBA Objective

Related CS-MARS Reports & Tools

GLBA Report Requirements: Access Control, Incident & Case Detail, Use of Network Services, SEM Audit Controls, Transmission Security, Workstation Use

GLBA Objective	Related CS-MARS Reports & Tools
Access Control	GLBA Report Requirements: Access Control, Incident & Case Detail, Use of Network Services, SEM Audit Controls, Transmission Security, Workstation Use Activity: Database Login Failures - All Events Activity: AAA Failed Auth - All Events Activity: AAA Based Access Failure - All Events Activity: Host Login Failures - All Events Activity: Host Login Failures - Top Destinations Activity: Host Login Failures - Top Users Activity: Host Privilege Escalation - All Events Activity: Remote Access Login Failures - All Events Attacks: Password - All Events Attacks: Privilege Escalation Failures - All Events Attacks: Password - Top Destinations
Incident and Case Detail	Attack: All - Top Rules Fired Incident TAB - GUI - Choose time period Case Management TAB - Case Details All Matching Sessions - Any Confirmed Positive Firing Event

	Network Status Page - Top Rules Fired
Use of Network Services	<p>Attacks: SANS Top 20 - Top Event Types</p> <p>Attacks: Database Server - Top Event Types</p> <p>Attacks: Web Server/App - Top Event Types</p> <p>Attacks: Login Services - Top Event Types</p> <p>Attacks: Mail Server - Top Event Types</p> <p>Attacks: RPC Services - Top Event Types</p> <p>Attacks: FTP Server - Top Event Types</p> <p>Activity: IDS Evasion - Top Event Types</p> <p>Attacks: Identity Spoofing - Top Event Types</p> <p>Attacks: Network DoS - Top Event Types</p> <p>Activity: Stealth Scans - Top Sources</p> <p>Activity: Scans - Top Destinations</p> <p>Activity: Scans - Top Destination Ports</p> <p>Activity: All Event and Netflow - Top Destination Ports</p> <p>Summary Page - All Events and Netflow</p> <p>Custom Query/Report based upon any Network Service</p>
SEM Audit Controls	<p>Admin>System Maintenance>View the Audit Trail</p> <p>Select - User or User Group for report -> Time based report</p> <ul style="list-style-type: none"> - Unsuccessful & Successful Logins - Db modifications - User actions & changes & notifications
Transmission Security	Activity: All - Top Reporting Device Types

	Activity: All - Top Reporting Devices
	Attacks: All - Top Destinations
	Attacks: All - Top Sources
	Activity: Network Usage - Top Destination Ports
	Activity: Network Usage Inbound - Top Ports
	Activity: Network Usage Inbound - Top Destinations
	Activity: Network Usage Outbound - Top Ports
	Activity: Network Usage Outbound - Top Destinations
	Activity: Denies Inbound - Top Destination Ports
	Activity: Denies Inbound - Top Destinations
	Activity: Denies Inbound - Top Sources
	Activity: Denies Outbound - Top Destination Ports
	Activity: Denies Outbound - Top Destinations
	Activity: Denies Outbound - Top Sources
	Activity: Attacks Prevented - Top Reporting Devices
	Resource Utilization: Concurrent Connections - Top Devices
Violation by Rule	Attacks: All - Top Event Types
	Attacks: All - Top Event Type Groups
	Attacks: All - Top Rules Fired
	Activity: All Activity reports
	Customer Report based upon Customer Created Rules
	Summary > Network Status Tab > Incidents Graph
	Summary > Network Status Tab > Top Rules Fired Graph
	Summary > Network Status Tab > Top Event Types Graph
Workstation Use	Activity: Host Login Failures - All Events
	Activity: Host Login Failures - Top Destinations
	Activity: Host Login Failures - Top Users
	Activity: Security Posture Not Up To Date - All Events
	Activity: Security Posture Not Up To Date - Top Users

	Activity: Security Posture Up To Date - Top Users
	Activity: Security Posture Validation Failure - Top Users
	Activity: Security Posture w/o Credentials - Top Hosts
	Activity: Spyware - Top Hosts
	Activity: Host Registry Changes - All Events
	Activity: Host Security Policy Changes - All Events
	Activity: P2P Filesharing/Chat - Top Hosts
	Activity: Spyware - Top Hosts
	Activity: IRC Activity - Top Hosts
	Activity: Covert Tunnels - Top Hosts
	<i>Any Activity Report - Hosts</i>