

SAN EMC Symmetrix Storage Array Standard Build Documentation

Version # 2
Date: August 28, 2006

Citigroup INTERNAL

TABLE OF CONTENTS

1	STANDARD BUILD IDENTIFICATION.....	3
1.1	CSB OVERVIEW	3
1.2	CSB GENERAL DESCRIPTION	4
1.3	AUDIENCE AND RESPONSIBILITIES	4
1.4	TERMINOLOGY, CONVENTIONS AND ASSUMPTIONS	5
1.5	BUILD OFFERING.....	6
1.6	DEPLOYMENT PLAN.....	7
1.7	FUTURE PLANS	7
1.8	CONTACTS.....	7
2	MANAGEMENT OVERVIEW	8
2.1	RISK CRITICALITY	8
2.2	INVENTORY LOCATION	9
2.3	TRAM/CAP/RA REFERENCES.....	10
2.4	MAKER/CHECKER, RECONCILIATION, AND AUDIT LOG REVIEW	10
2.5	SELF ASSESSMENT PROCEDURES	11
3	TECHNICAL OVERVIEW.....	12
3.1	COMPONENT INTERACTION	12
3.2	BUILD SPECIFICATIONS	14
3.3	ARCHITECTURE/NETWORK TOPOLOGY	15
3.4	SCALABILITY.....	16
3.5	PERFORMANCE METRICS.....	16
4	SYSTEM INSTALLATION.....	17
4.1	PRE-INSTALLATION CHECKLIST	17
4.2	INSTALLATION METHODS.....	17
4.3	INSTALLATION PARAMETER SETTINGS	18
4.4	INSTALLATION CHECKLIST.....	18
5	SYSTEM CONFIGURATION	19
5.1	SYSTEM SETTINGS.....	19
5.2	SECURE TOPOLOGY	19
5.3	NETWORK PROTOCOLS/PARAMETERS/SETTINGS.....	19
5.4	ADDITIONAL PARAMETERS/SETTINGS.....	19
5.5	SYSTEM CONFIGURATION CHECKLIST.....	20
6	SECURITY CONFIGURATION	21
6.1	PRODUCT/CUSTOMER DATA CLASSIFICATION	21
6.2	IDENTIFICATION AND AUTHENTICATION	21
6.3	CONFIDENTIALITY AND INTEGRITY	23
6.4	AUTHORIZATION AND ACCESS CONTROL	24
6.5	INCIDENT RESPONSE AND INTRUSION DETECTION	25
6.6	ACCOUNTABILITY	25
6.7	AVAILABILITY	26
6.8	BANNER PAGE.....	26
6.9	SECURITY CONFIGURATION STEP-BY-STEP CHECKLIST.....	26
6.10	COMPENSATING CONTROLS	26
7	OPERATIONAL PROCEDURES.....	28
7.1	OPERATIONAL SUPPORT GUIDE.....	28
7.2	MAINTENANCE/CHANGE CONTROL/COB.....	28

7.3	EMERGENCY PROCEDURES/TROUBLESHOOTING	29
7.4	LEVEL III PROCEDURES	29
7.5	ASSET MANAGEMENT	30
8	SUPPORTING DOCUMENTATION / REFERENCES	31
8.1	ADMINISTRATIVE GUIDES	31
8.2	USER GUIDES	32
8.3	VENDOR DOCUMENTATION	32
8.4	INDUSTRY STANDARDS	33
8.5	SELF ASSESSMENT GUIDE	33
8.6	SAMPLE AUDIT LOGS	33
	APPENDIX A: DOCUMENT REVISION HISTORY	35
	APPENDIX B: STANDARD AUDIT PROGRAM (SAP) / TAILORED REVIEW PROGRAM (TRP)	36
	APPENDIX C: VULNERABILITY ASSESSMENT REPORT	37

1 STANDARD BUILD IDENTIFICATION

The Citigroup SAN EMC Symmetrix Storage Array Standard Build describes all of the features, software, protocols, parameters, etc. that are necessary to provide a stable, secure platform for all global SAN EMC Symmetrix Storage Array systems at Citigroup. This document sets the security standard for all SAN EMC Symmetrix Storage Array systems at Citigroup. This Standard Build provides Infrastructure Security Classification Class 'C' services, which protect against "threats from entities with internal network access, where a 'casual user' utilizing penetration utilities and tools can accomplish the attack".

1.1 CSB OVERVIEW

Document Author:	Vivek Jain
Author Org Type:	Distributed Engineering
Author Phone Number:	908 563-0019
Author Email Address:	Vivek1.jain@citigroup.com
Author Department Name:	Global Distributed Storage Engineering
Document Location:	Documentum
Global Standard Build Owner Agreement:	Christian Parker-Lentz
Global Standard Build Operational Owner Agreement:	Paul Stemmler
Revision History:	See Appendix A

1.1.1 Citigroup Standard Build Identification

Official Standard Build Name and Acronym:	SAN EMC Symmetrix Storage Array Standard Build
Product Name (s), Acronym(s), and Version(s):	Symmetrix 8730, 8830, Symmetrix DMX 1000, 2000, 3000, DMX-3; Solutions Enabler; SymmRemote, WWDS, PowerBroker, eTrust
Other:	

1.1.2 Citigroup Build Product Owner

Global Standard Build Product Owner:	Eliot Wilson
Standard Build Product Owner Department Name:	Global Distributed Storage Engineering
Region(s) (if applicable):	CTI Asia Pacific, CTI EMEA, CTI Latin America, CTI Mexico, CTI North America, CTI Japan
Other:	

1.1.3 Citigroup Standard Build Operational Owner

Global Standard Build Operational Owner:	Paul Stemmler
Standard Build Operational Owner Department Name:	Global Storage Management Group
Region(s) (if applicable):	CTI Asia Pacific, CTI EMEA, CTI Latin America, CTI Mexico, CTI North America, CTI Japan
Other:	

1.2 CSB GENERAL DESCRIPTION

The SAN EMC Symmetrix Storage Array offers block access storage to application servers over the Fibre Channel (FC) network using the SCSI protocol. The Symmetrix arrays can be managed in-band, via the fiber channel network, or out-of-band, via the TCP/IP interface. The Service Processor within the array allows vendor personnel to carry out initialization, advanced configuration and diagnostics on site or from a remote support center.

1.3 AUDIENCE AND RESPONSIBILITIES

This document is appropriate for all compliance, auditing, operational, technical, and business application groups who install, configure, operate, or audit the EMC Symmetrix Storage Array in a SAN environment. The information compiled in this document has been tested and certified by Global Distributed Storage Engineering (GDSE). For additional information, please email GDSE at *GT *Global Distributed Storage Engineering* or gdse@citigroup.com

1.4 TERMINOLOGY, CONVENTIONS AND ASSUMPTIONS

FC	Fibre Channel
GDSE	Global Distributed Storage Engineering
GSMG	Global Storage Management Group
HBA	Host Bus Adapter. Hardware-based Fibre-channel adapter card that enables host connectivity to the Storage array via the SAN.
LUN	Logical Unit Number is the number given to the logical disk devices in a storage array.
PCM	Process Control Manual: a collection of Level 3 Procedures that are step by step procedural documents which outline how a unit performs roles, responsibilities, activities, and/or function(s). Contingent on the roles and responsibilities performed by a unit, the level 3 can be completely aligned (e.g. Change Management Function) to one CITMP topic or aligned with multiple CITMP topics based on the function(s) performed (e.g. Data Center Operations). A Level 3 is not a user guide for a particular application or a vendor provided manual, such as a configuration guide. While these types of documents may enhance the overall understanding of a particular function/ operation, they should only be referenced in the Level 3 (i.e. appendix or url address).
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network. This is a network topology for block-based storage arrays connected to application servers via network switches most commonly based on Fibre-channel (FC) network protocol.
SCSI	Small Computer System Interface
Solutions Enabler	It is a suite of software tools to configure and manage the Symmetrix array
Storage Array	A storage array is a RAID-based storage system providing high capacity, availability, integrity, performance and disaster recovery services for stored data.
SYMACL	Symmetrix Access Control List is a function of Solutions Enabler to control access to the configuration and management functions.
SYMAPI	Symmetrix Application Programming Interface
Symmetrix	EMC high-end storage array
TRAM	Technology Risk Assessment Matrix
VCMDB	Volume Control Masking Database is a disk device on the Symmetrix that holds the access information of LUNS by various hosts. It is a security mechanism that allows access to LUNs by authorized hosts only.
VTM	Vulnerability and Threat Management

WWDS	World Wide Dial Services
------	--------------------------

1.5 BUILD OFFERING

The SAN EMC Symmetrix Storage Array Standard Build contains the following components.

- A pre-configured EMC Symmetrix Storage Array based on GDSE-certified Engenuity Microcode and standard Bin-file configuration for Symm 8000 and DMX series.
- A Solutions Enabler management station, which is connected in-band (via FC) to the storage array. The management station is an SOE Solaris or Windows workstation configured with Solutions Enabler application.
- Remote fault monitoring application(s) installed on the vendor-controlled Symmetrix Service Processor.

1.5.1 Build Offering Definitions

CSB Component	Define Component (Intent)	Version	CSI # (if applicable)	End of Life	Owner
Symmetrix DMX	Storage Array	1000, 2000, 3000, DMX-3		TBD	TIE /Robert Small
DMX Engenuity microcode	Operating System	5670,5671, 5771		TBD	TIE /Robert Small
Symmetrix 8000	Storage array	8530,8730, 8830		TBD	TIE /Robert Small
8000 Engenuity microcode	Operating system	5567, 5568			TIE /Robert Small
Solutions Enabler	Configuration and Management	6.X.X		TBD	TIE /Robert Small
EMC , Symm Remote, WWDS, eTrust	Remote fault monitoring and management	Based on Symm Microcode			EMC
PowerBroker	Secures user access to Solutions Enabler CLI.	SAN			

Please refer to the online [GDSE support matrix](#) for latest certified versions. If the certified versions are different than listed above, please refer to the respective Solution guide document.

1.6 DEPLOYMENT PLAN

1.7 FUTURE PLANS

No major changes to the current release or new builds are planned in the short term. Any new CSBs will be based on the availability of new products from the vendor and certification by GDSE.

1.8 CONTACTS

The head of Distributed Engineering has information ownership of SAN products and all related engineering documents. SAN products are available in the Citigroup Technology Catalogue. All security and technology best practices for SAN products are the responsibility of Global Distributed Storage Engineering.

1.8.1 Contact Definitions

External Contact/ Vendor	Contact Phone/Email	Maintenance Agreement and Support	Technical Product Manager	Operational Support Owner
Stephanie Lubrano/EMC	800-SVC-4EMC 508-435-1000 Lubrano_Stephanie@emc.com	24 x 7 Support	Ron Parmar	Scott Goellner

Internal Contact	Organization	Function	Phone Number/Email
Christian Parker-Lenz	Global Platforms and Storage Engineering	Dept Manager	908-563-0022 christian.parkerlentz@citigroup.com
Robert Small	GDSE	Dept. manager	817-317-8216 Robert.small@citigroup.com
John Hegarty	Global Storage Management Group	Director, operations	212-723-5279 john.m.hegarty@citigroup.com

2 MANAGEMENT OVERVIEW

2.1 RISK CRITICALITY

2.1.1 Risk Assessment

Product	High	Medium	Low
Symmetrix DMX	☐	☒	☐
DMX Enginuity microcode	☐	☒	☐
Symmetrix 8000	☐	☒	☐
8000 Enginuity microcode	☐	☒	☐
Solutions Enabler	☐	☒	☐
EMC Symm Remote, Citigroup WWDS	☐	☒	☐

2.1.2 Define Standard Build Criticality

CSB Name	Infrastructure Classification Component?
Symmetrix DMX	Yes
DMX Enginuity microcode	Yes
Symmetrix 8000	Yes
8000 Enginuity microcode	Yes
Solutions Enabler	Yes
EMC Symm Remote, Citigroup WWDS	Yes

2.1.3 Threat Scenarios

Threat Scenarios	Applicable?
Unauthorized disclosure, modification, or destruction of information	☒

Threat Scenarios	Applicable?
Inadvertent modification or destruction of information	☒
Non-delivery or misdelivery of service	☒
Denial or degradation of service	☒
Impersonating, misusing, or false acknowledgements of a user or system	☐
Eavesdropping	☐
Replay or reorder of messages or information	☒
Denial or origin, submission, delivery	☐
Masquerading	☐
Repudiation	☐
Other	☐

The above listed threat scenarios are mitigated by requiring SOE user logins with strong passwords and audit trail reviews to determine that users are acting properly. User roles and privileges are based on their respective functions. Refer to the SAN Product TRAM and CAP documents for more information. FC switches are networked as a private switched fabric and are not connected to the corporate IP network. Hence, DoS and replay attacks are not applicable in this environment.

2.2 INVENTORY LOCATION

Information on SAN-produced inventories is maintained within the [SAN-Resource Management PCM](#). For details see the [Storage Report January 2005](#).

2.3 TRAM/CAP/RA REFERENCES

Product	TRAM / CAP / RA ?	CAP / RA Reference #:	Date Completed	Author	Author Contact Information
SAN EMC Symmetrix storage array	IS Product TRAM	SAN IS Product TRAM v1	03/29/04	Eliot Wilson	212-816-7258
Symm Technical TRAM	Technical TRAM	GDSE-04006-TRAM	05/12/04	Eliot Wilson	212-816-7258
SAN EMC Symmetrix storage array	RA	CTI-2004-251		Parul Jain	908-563-3136
SAN EMC Symmetrix storage array	CAP	8738-PRAN	07/31/05	Parul Jain	908-563-3136

RA CTI-2004-251 - The scope of this risk acceptance is limited to deficiencies identified in the "Product Owner" sections within the IS Product TRAM for SAN. Regional Operations teams are expected to create their own Risk Acceptance to cover any gaps identified in the "Operational Owner" sections within the IS Product TRAM, as well as gaps identified in other CITMP TRAMS.

CAP 8738-PRAN - Monitoring and reconciliation of SAN management activity is only possible if the management applications record user actions. Most SAN management applications either do not record user actions or only record partial information, which is not sufficient for reconciliation. Because Citigroup does not have access to the source code for these applications, Citigroup has to rely on the vendor to fix their products. Even as Citigroup is following up with the vendor, the corrective action being proposed is to assess the technical feasibility of using or building software applications that can compensate for some of the deficiencies in the SAN management applications. If it is found to be technically feasible, the plan commits to engineering of the solution and making it ready for global deployment.

CAP 8738-PRAN has been completed and closed. [PowerBroker](#), [eTrust Audit](#) and [SANscreen](#) are new tools that are implemented as compensating controls.

2.4 MAKER/CHECKER, RECONCILIATION, AND AUDIT LOG REVIEW

Refer to section 3.2 of Procedures of [SAN Information Security PCM](#).

Function	Responsible Party
Maker/Checker	GSMG / GDSI
Security Audit Log Review & Reconciliation	GDSI
Operational Support Functions	GSMG

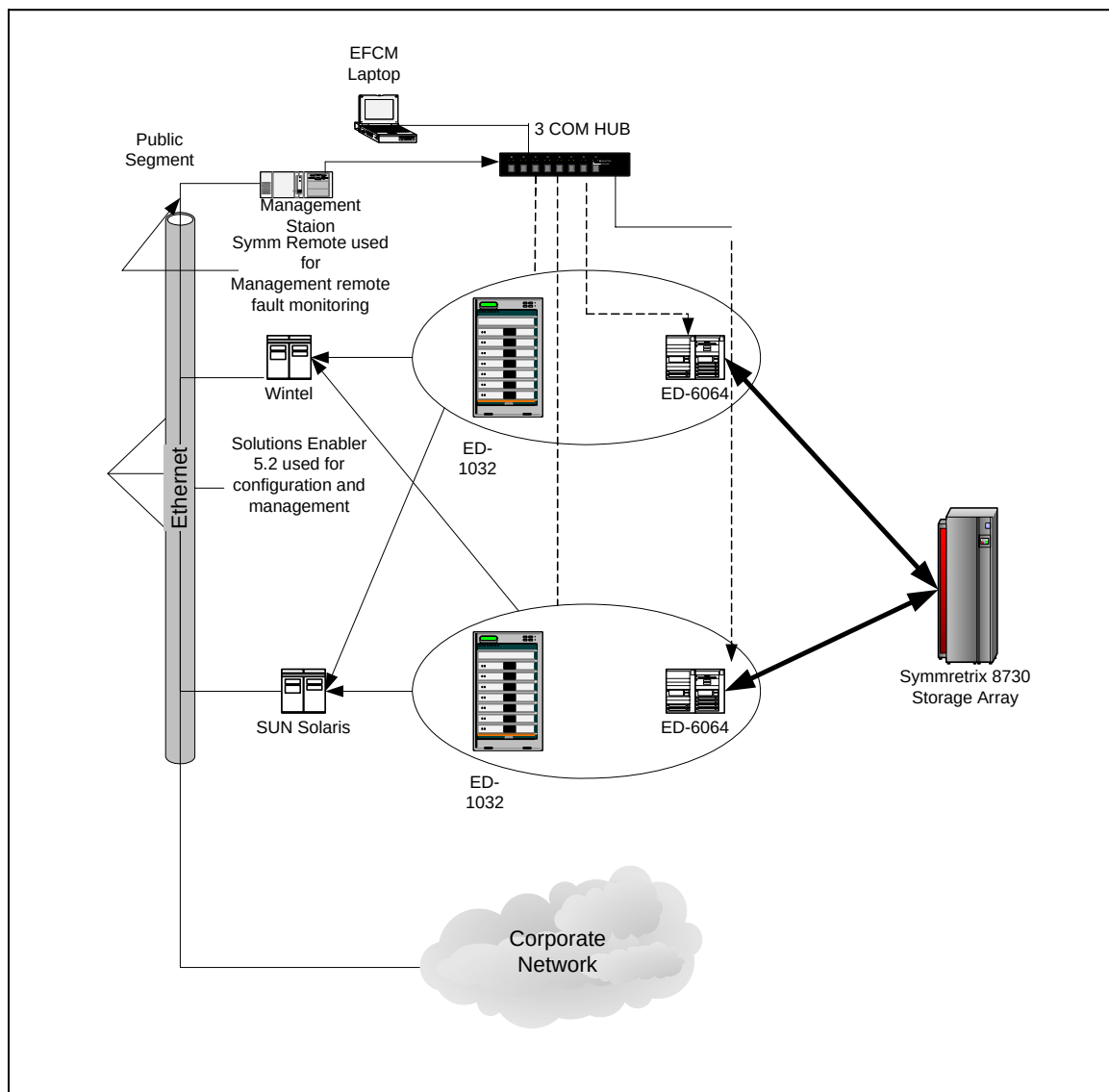
2.5 SELF ASSESSMENT PROCEDURES

The SAN EMC Symmetrix Storage array product follows all Global Compliance self-assessment rules and regulations. The Distributed Storage Engineering group that manages the SAN EMC Symmetrix Storage array performs all technical TRAMs, log reviews and other procedures to keep up with releases, patches, etc.

3 TECHNICAL OVERVIEW

3.1 COMPONENT INTERACTION

The Symmetrix Storage Array operates in a SAN environment, in which it is logically connected to various application servers via FC switches. The Symmetrix Storage Array itself is composed of 3 different sub-components, namely, the Storage Array with a certified version of Operating system, a management station for configuring and managing the Storage Array, and a vendor-controlled remote fault-management system.



3.1.1 Storage Array

The Symmetrix Array offers block access storage to hosts over the FC network using the SCSI protocol. The Symmetrix arrays can only be managed in-band, via a management station connected over the fibre-channel network. The Remote fault-management system is resident on a Service Processor within the array that allows vendor personnel to carry out initialization, advanced configuration and diagnostics on site or from a remote support center. The storage array is configured according to GDSE-certified bin-file standards, as described below.

- EMC Symmetrix DMX - supports the current distribution of Symmetrix devices across two pairs of fiber-channel directors.
Every 2 pairs of FAs, that make-up the EMC rule 17 pairing, define a storage segment within the BIN File.
 - o i.e. Symmetrix DMX1000 is made up of 4 to 8 storage segments.
 - o i.e. Symmetrix DMX 2000 is made up of 8 to 12 storage segments.

GDSE Engineering maintains this Information in Section 12, “LUN Distribution” of the [EMC Symmetrix DMX Solutions Guide](#) (GDSE 03038-B) document.

- EMC Symmetrix 8000 family - All LUNS are pre-mapped behind dedicated FA ports. In a 2-port FA Symmetrix configuration, a LUN is assigned to 2 independent FA ports. In a 4-port FA configuration, a LUN is assigned to 4 independent FA ports. This type of grouping is seldom referred to as segments and should always follow an odd/even pairing.

GDSE Engineering maintains this information in Section 12, “LUN Distribution” of the [EMC Symmetrix 8000 Best Practice Guide](#) (GDSE 03031-B).

3.1.2 Management Station

The DMX Storage Array operates in a SAN environment, in which it is logically connected to various application servers via FC switches. The DMX Storage Array itself is composed of 3 different sub-components, namely, the Storage Array with a certified version of operating system, a management station for configuring and managing the storage array, and a vendor-controlled remote fault-management system. An explanation of the management station is depicted in section 3 of the [Solutions Enabler Certification - Solaris](#) document. The DMX Storage Array operates in a SAN environment, in which it is logically connected to various application servers via FC switches. The DMX Storage Array itself is composed of 3 different sub-components, namely, the Storage Array with a certified version of operating system, a management station for configuring and managing the storage

Citigroup INTERNAL

array, and a vendor-controlled remote fault-management system. An explanation of the management station is depicted in section 3 of the [Solutions Enabler Certification - Solaris](#) document.

3.1.3 Remote Management

An explanation and diagram of the remote management station is depicted in section 11 of the [EMC Symmetrix DMX Solutions Guide](#) (GDSE 03038-SG) document.

3.2 BUILD SPECIFICATIONS

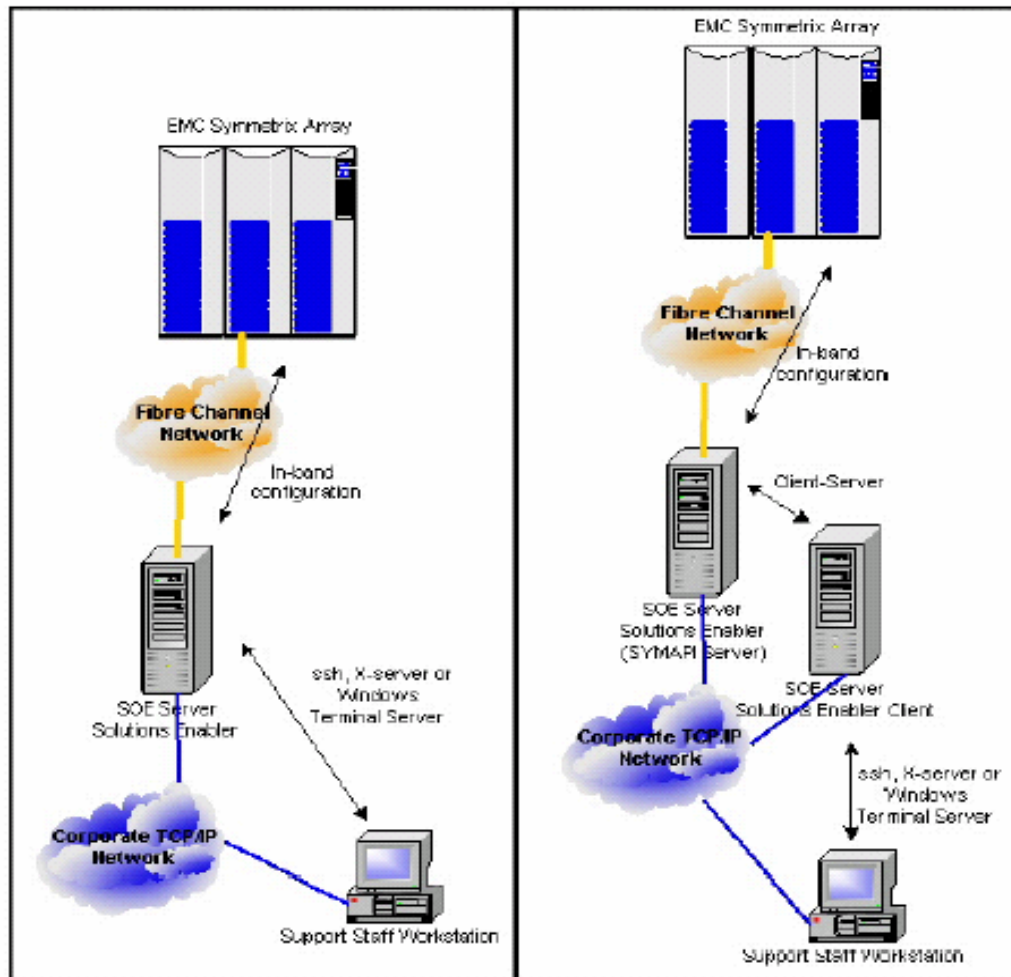
Component Type	Standard Build Component	Purpose	Vendor	Version
Hardware:	Symmetrix DMX Symmetrix DMX	Block Base Storage	EMC EMC EMC	1000 2000 3000 DMX-3
	Symmetrix 8000 Symmetrix 8000	Block Base Storage	EMC EMC	8530 8730 8830
Software:	Solutions Enabler	Configuration and Management	EMC	6.X.X
Operating Systems:	DMX Enginuity Microcode	Array Operating System	EMC	5670, 5671, 5771
	8000 Enginuity Microcode – 8730 8000 Enginuity Microcode – 8830	Array Operating System Array Operating System	EMC EMC	5567, 5330 5568m 6726
Supporting Products:	EMC, DIAL SYMMREMOTE, SYMMIP	Remote Fault monitoring and management	EMC	Based on Symm Microcode
	PowerBroker	Secures user access to Solutions Enabler CLI.		SAN

3.2.1 When to use standard build offering

This standard build is to be used for installation, administration and maintenance of all global storage components in a secure configuration.

3.3 ARCHITECTURE/NETWORK TOPOLOGY

GDSE Engineering maintains this information in the access, audit and security sections of the [EMC Symmetrix DMX Solutions Guide](#) (GDSE 03038-SG) document.



3.3.1 Symm Remote

The SymmRemote application do not process any business information. In order to protect passwords, link encryption should be enabled. For more information, refer to section 15 (Vendor remote access to Symm) of the [EMC Symmetrix DMX Solutions Guide](#).

3.4 SCALABILITY

The table below shows the hard-disk drive scalability of the DMX Symmetrix Storage Array. Based on the drive configuration, there is a corresponding scalability of other components, such as cache memory and Fiber-ports.

Drive Size	DMX Model	Physical Disk Devices	Available Disk Devices RAID1	Usable Open Systems Storage Capacities (GB ₁₀)
73GB	1000	72 to 144	36 to 72	2,628 to 5,256
	2000	144 to 288	72 to 144	5,256 to 10,512
146GB	1000	72 to 144	36 to 72	5,256 to 10,512
	2000	144 to 288	72 to 144	10,512 to 21,024

For more information, see section 10 of the [EMC Symmetrix DMX Solutions Guide](#) document.

The scalability of Symmetrix 8000 is as follows.

- Maximum number of 73GB drives supported on Symmetrix 8000 family: 258
- Recommended number of splits on a 73GB drive: 8 (see bin file configuration)
- Recommended number of spare disks: 2 (already included in 258)
- Recommended split sizes per physical disk: 4x14.88GB₁ + 4x2.06GB₂ = 8

Refer to the section titled “Hardware Configuration” in the [EMC Symmetrix 8000](#) (GDSE-03001-B) document.

3.5 PERFORMANCE METRICS

Certain aspects of performance management can be monitored by the Operating System, HBA-based tools such as sar, prstat, powermt, etc. They monitor the disk and path performance as seen by the host. In certain scenarios, performance monitoring and management activities are performed by EMC specifically when storage management requires them.

Comprehensive performance-management tools are being evaluated for future certification. This document will be updated as, and when, a tool is certified by GDSE and implemented in the environment.

4 SYSTEM INSTALLATION

4.1 PRE-INSTALLATION CHECKLIST

EMC Symmetrix DMX Storage Array system requirements for installation are contained in Sections 8.1 and 8.2 of the [EMC Symmetrix DMX Solutions Guide](#) document.

EMC Symmetrix 8000 storage array family system requirements for installation are contained in the section labeled “Hardware Configuration” of the [EMC Symmetrix 8000](#) document.

EMC Solutions Enabler system requirements for installation are contained in the [EMC Solutions Enabler Solutions Guide](#)

Management Stations system requirements for installation are contained in Section 7, “Management Station,” of the [EMC Symmetrix 8000](#) document.

4.2 INSTALLATION METHODS

4.2.1 STORAGE ARRAY INSTALLATION METHODS

Physical and environmental setup of all enterprise storage arrays should conform to vendor specifications and facilities provided by the GDSE Engineering planning group.

Rack mount	Not Applicable
Power DMX Environmental Requirements	DC Hardware Planning
Cooling DMX Environmental Requirements	DC Hardware Planning
Cabling DMX Environmental Requirements	DC Hardware Planning

GDSE Engineering maintains this information in Section 7.2 of the [EMC Symmetrix DMX Solutions Guide](#) document.

4.2.2 SOLUTIONS ENABLER INSTALLATION METHODS

The EMC Solutions Enabler installation procedure installs the client/server application (symapisrv) in the bin directory. The procedure also installs three files (netcnfg, symapinlck, and symapislck) in the configuration directory (/var/symapi/config). On both the client host and server host, the editable netcnfg

file lists the network services available from that local host or from one or more remote hosts. The symapinlck and symapislck files are internal, used by the server as lock files on a server host to guarantee a single port listener for a network service. Do not delete or alter these lock files.

GDSE Engineering maintains this information in Section 9 of the [EMC Solutions Enabler Solutions Guide](#).

4.3 INSTALLATION PARAMETER SETTINGS

See [section 4.4](#) - Installation Checklist.

4.4 INSTALLATION CHECKLIST

4.4.1 Installing the Symmetrix Storage Array Hardware and Solution Enabler

Step #	Task	Completed Y/N?
1	The vendor installs the Symmetrix Storage Array with GDSE certified Microcode	
2	The vendor performs checkout	
3	Install Solutions Enabler software (as SYMAPI server) in the machine designated as the SAN management station, according to the procedures described later in section 8 of the EMC Solutions Enabler Solutions Guide .	
4	Install the same Solutions Enabler software (as SYMAPI client) on the client machine.	
5	Invoke symlmf and apply the SYMAPI Server license key.	
6	Install Powerbroker client on the SAN control workstation.	

5 SYSTEM CONFIGURATION

5.1 SYSTEM SETTINGS

5.1.1 Physical storage array system settings and configuration

For storage array hardware, the following types of settings must be configured.

- Hardware configuration
- Bin File configuration
- LUN distribution

For the Symmetrix DMX physical system settings, see the following sections in the [EMC Symmetrix DMX Solutions Guide](#) document.

- Chapter 8 “SOE Symmetrix DMX Standard Hardware Configurations”
- Chapter 9 “SOE Symmetrix DMX Bin File Configuration”
- Chapter 12 “LUN Distribution”

For the Symmetrix DMX physical system settings, see the following sections in the [EMC Symmetrix 8000](#) document.

- Section named “Hardware Configuration”
- Section named “Bin File Configuration”
- Section named “LUN distribution”

5.1.2 Solution Enabler Software Configuration Settings

For the Solutions Enabler system settings, see [Section 5.5](#) - Solutions Enabler Configuration Checklist.

5.2 SECURE TOPOLOGY

For the Symmetrix secure topology, see [Section 3.3](#) - Architecture/Network Topology .

5.3 NETWORK PROTOCOLS/PARAMETERS/SETTINGS

For the network protocols, parameters, and settings, see the physical and system settings in [Section 5.1](#) - System Settings .

5.4 ADDITIONAL PARAMETERS/SETTINGS

There are no additional parameters and settings for the Symmetrix array.

5.5 SYSTEM CONFIGURATION CHECKLIST

Procedures for configuring the Solutions Enabler software

After completing the installation of the Solutions Enabler, configuration parameters must be set on the SYMAPI server and SYMAPI client before using the Solutions Enabler SYMCLI commands.

The following configuration steps must be completed.

Step #	Task	Completed Y/N?
1	Set the CLI path. .	
2	Edit the netcnfg file.	
3	Set the SYMAPI server and client environment variables.	
4	Build the symapi database. .	

Please refer to the [EMC Solutions Enabler Solutions Guide](#).

6 SECURITY CONFIGURATION

6.1 PRODUCT/CUSTOMER DATA CLASSIFICATION

The SAN is infrastructure, and thus will be managed towards a class 'C' certification. Therefore, the SAN can process and store information classified as "public", "internal" and "confidential" only. Information classified as "restricted" or "highly confidential" cannot be processed on the SAN unless adequate controls, such as encryption, are built into the application. It is the responsibility of the businesses to encrypt any data with a classification higher than confidential.

6.2 IDENTIFICATION AND AUTHENTICATION

The tools that make up the Solutions Enabler product do not authenticate or authorize users. As a compensating control, the tools should only be accessible after authentication against an SOE server (SAN management station). This is enabled by the topology illustrated in [Section 3.3](#) - Architecture/Network Topology. SYMACL is a component of the Symmetrix product that provides the ability to setup and maintain an access control capability over Solutions Enabler and Symmetrix resources. SYMACL restricts which hosts are authorized to manage Symmetrix resources, and which SAN resources they are authorized to manage.

6.2.1 Adding/Deleting Users and Groups

Groups are created in SYMACL to restrict Solutions Enabler command access to manage access to physical storage arrays. To set up an access control group, you need to create a group and then various access IDs of the hosts and users as members of that group. Network administrators create users in the SOE OS environment. Refer to the Solaris and Windows 2000 Server Standard Builds.

For details, refer to sections 11.3.2.1 and 11.3.2.3.1 of the [EMC Symmetrix DMX Series Solutions Guide](#)

6.2.2 Authentication Method(s)

6.2.2.1 Physical Storage Array Authentication (for DMX 1000, 2000, 3000, DMX-3, Symm8000 Family)

The Storage Array identifies hosts by the World Wide Name ("WWN") of the host HBA. The array does not authenticate the identity of the hosts. To compensate, the fibre channel network that provides access to the array must not expand beyond a secure data center.

Because the identification and authentication mechanisms on the TCP/IP interface are unknown, it should not be connected to a private or public TCP/IP network. Instead, all management tasks should be carried out in-band, through the fiber channel network.

For more information, refer to section 11.2 of the [EMC Symmetrix DMX Series Solutions Guide](#).

6.2.2.2 Solution Enabler Authentication

The tools that make up the Solutions Enabler product do not authenticate or authorize users. As a compensating control, the tools should only be accessible after authentication against an SOE server (via the SAN management station).

For more information, refer to section 12.2 of the [EMC Symmetrix DMX Series Solutions Guide](#).

6.2.2.3 Remote Fault Management Authentication

Symm-Remote is not capable of identifying users or using dynamic tokens for authentication. It supports only one user ID that is used by all vendor support staff. Symm-IP improves on the identification capabilities of Symm-Remote by limiting access to hosts installed in the vendor support center by use of digital certificates. Also, because the calls are expected to only originate from the vendor support center, the PBX can be programmed to reject calls coming from all other numbers. GDSE and Network Security Engineering certify the Remote fault-management solution in accordance with CISS.

For more information, refer to section 15.2 of the [EMC Symmetrix DMX Series Solutions Guide](#).

6.2.3 Password Policies and Controls

SAN management stations are built to SOE standards, and the system administrators and information security teams enforce password policies and controls. Refer also to the SSM and Windows 2000 Server Standard Builds.

6.2.4 Functional ID Controls

There are no functional IDs on the storage array, since it can only be accessed via the service processor or the management station. The only functional IDs on the service processor are used for Symm-Remote and

are controlled by the hardware vendor (EMC). The management station uses the SOE user IDs for authentication.

As a compensating control for the functional IDs, a new Symmetrix vendor remote access has been architected where access to Symm-Remote is restricted via a single-use password via a Safeword session that is documented in detail in the following document.

http://www.citigroup.net/tie/neteng/external/wwds/EMC_Solution_5.doc.

6.2.4.1 Functional ID Security

See [section 6.2.4](#) - Functional ID Controls.

6.3 CONFIDENTIALITY AND INTEGRITY

6.3.1 Virus Protection

SOE provides virus protection for the Management station.

6.3.2 Encryption

6.3.2.1 Internal to product

The only encryption used within components of the Symmetrix product is within the Symm-Remote component, which is used for remote vendor diagnostics, where a proprietary 40-bit encryption is used. As a compensating control for the encryption gap, a new Symmetrix vendor remote access has been architected, where access to Symm-Remote is restricted via a single-use password via a Safeword session that is documented in detail in the following document.

http://www.citigroup.net/tie/neteng/external/wwds/EMC_Solution_5.doc.

Note: The 40-bit encryption issue is also addressed in **RA CTI-2004-251**.

6.3.2.2 Encryption Algorithms Used (if any)

Encryption of user data is a function of the Application server. Applications are not executed in the SAN environment. No user IDs or passwords are stored on the storage array.

6.3.3 Data Storage

Encryption of data is the responsibility of the business.

6.3.4 Data Transmission

This is a data storage product and stores and transmits the data in its native format as received by the array.

6.4 AUTHORIZATION AND ACCESS CONTROL

Physical Storage

The physical array offers the following 3 controls.

1. Access to storage within the array - VCMDB
2. Access to entries within the VCMDB - VCMDB Access Control
3. Access to array configuration - SYMACL

For more information, refer to section [Section 14: Symmetrix DMX Security](#) of DMX Best practices.

Solutions Enabler Authorization:

Solutions Enabler does not identify users and therefore does not have any access control capabilities. Access to the tool is restricted by hosting the application on an SOE server that has been authorized to access the Symmetrix with SYMACL. Logon to this SOE server should be limited to staff authorized by Storage Management. As a compensating control, PowerBroker should be installed on the SAN Management stations.

For more information, refer to section 8 of [PowerBroker Implementation for SAN](#) (GDSE-05006-S).

Remote Fault Management:

Symm-Remote and Symm-IP do not have any access control capabilities. The vendor manages this for diagnostics and maintenance purposes. Symm-Remote and Symm-IP are installed on the service processor that is isolated from the corporate TCP/IP network. WWDS should be implemented for vendor remote access.

For more information, refer to section 15 (Vendor remote access to Symm) of the DMX Best Practices .

6.4.1 Entitlement Reviews

Information regarding this topic may be found in Section 3.1 of the [SAN-Information Security PCM](#).

6.4.2 Separation of Duties: System and Security Administrator Configuration

Information regarding this topic may be found in Section 6.4 of the [GSMG Information Security Baseline PCM](#).

6.4.3 File System Access Controls

See [Section 6.4.1](#), Entitlement Reviews, for details about File System Access Controls. The underlying OS file system is a part of the Standard Build for Solaris or Wintel builds and can be referenced in the links below.

6.5 INCIDENT RESPONSE AND INTRUSION DETECTION

No intrusion detection is used or required in this environment. It is protected by internal firewalls and is completely internal to the corporation. Information regarding this topic may be found in sections 5.1 of the [SAN-Information Security PCM](#).

6.5.1 Physical Storage

The array maintains a log of system administration activities. This log can be obtained by using the “symaudit” CLI command. See the [EMC Symmetrix DMX Series Solutions Guide](#) section 11.5 for more information. Refer to section 5.1 of the [SAN-Information Security PCM](#).

6.5.2 Solutions Enabler

This component does not generate any logs. System administration actions are recorded on the Symmetrix array instead. For more information, refer to Section 12.5 of the [EMC Symmetrix DMX Series Solutions Guide](#). Refer to section 5.1 of the [SAN-Information Security PCM](#).

6.5.3 Remote Fault Management

The Symm-Remote and Symm-IP applications track dial-in activity. For more information, refer to Section 15.5 of the [EMC Symmetrix DMX Series Solutions Guide](#). Refer to section 5.1 of the [SAN-Information Security PCM](#).

6.6 ACCOUNTABILITY

6.6.1 Auditing

GDSE Engineering maintains this information in the access, audit and security sections of the [DMX Solutions Guide](#) (GDSE 03038-SG) document.

6.6.1.1 *Turning on auditing, selecting auditing events*

GDSE Engineering maintains this information in the access, audit and security sections of the [DMX Solutions Guide](#) (GDSE 03038-SG) document.

6.6.1.2 *Audit Trail Reviews*

Information regarding this topic may be found in section 5.3 of the [SAN-Information Security PCM](#).

6.6.2 Maker/Checker

This product does not perform automated maker/checker. Information regarding the manual procedure may be found in Section 6.4 of the [SAN-Information Security PCM](#).

6.6.3 Reconciliation

This product does not perform automated reconciliation. Information regarding the manual procedure may be found in section 3.2 of the [SAN-Information Security PCM](#). Additional information on how to access the Symm audit logs is available in Section 6.6.1

6.7 AVAILABILITY

The Symmetrix Storage Array is designed and engineered to run 24x7. There are redundant paths from the host to the disks in the storage array. The disks are also mirrored to protect against a disk failure. For critical applications, the LUNs are configured to replicate data across geographically separated data centers. See section 8 of the [EMC Symmetrix DMX Solutions Guide](#) document.

6.8 BANNER PAGE

A banner page is not applicable for the Symmetrix Storage Array product. SOE provides the banner for the management console.

6.9 SECURITY CONFIGURATION STEP-BY-STEP CHECKLIST

For information about the Physical Array, refer to Sections 11.3.1 through 11.3.2.2 of the [EMC Symmetrix DMX Series Solutions Guide](#).

6.10 COMPENSATING CONTROLS

The [EMC Symmetrix DMX Series Solutions Guide](#) provides for the Solutions Enabler component only being installed on a SAN Control Workstation where users are authenticated with an SOE Windows or Solaris Standard build. Refer to Section 8 of the [SAN IS TRAM Supporting Evidence \(GSDA 04006-SE\)](#) document.

6.10.1 Procedures

GDSE Engineering maintains this information in the access, audit and security sections of the [DMX Solutions Guide](#) (GDSE 03038-SG) document.

6.10.2 Operational Approvals

The Global Storage Management Group Functional Area Manager gives operational approvals.

6.10.3 Compensating Control Procedures step-by-step checklist

Not Applicable

7 OPERATIONAL PROCEDURES

7.1 OPERATIONAL SUPPORT GUIDE

Operational support procedures are described in a series of Level III PCMs across CITMP domains. For more information, refer to [Section 8.1.3](#) - Operational Support Guides.

7.2 MAINTENANCE/CHANGE CONTROL/COB

7.2.1 Problem Management

Information on Problem Management processes, such as ticket creation, incident response, escalation; notification, prevention, and continuous improvement, are described in Section 3.2 of the [SAN-Problem Management PCM](#).

7.2.2 Change Control

Change control procedures, such as change identification, change approval, and change review, are described in the [SAN-Change Management PCM](#).

7.2.3 Internal, External, Vendor, Remote Access Procedures

Remote access procedures are described in Sections 3.8, 3.10, and 3.12 of the [SAN-Information Security PCM](#).

7.2.4 VTM/Patch updates

The Citigroup Vulnerability and Threat Management team follows a process based on the following [Corporate Information Security Standards](#).

§ 4.7.1. Only run operating systems and software that are currently supported by an approved vendor or have an active and appropriate release of patches and configuration updates available to address security issues,

§ 4.7.2. Apply all approved security patches and configurations within the time periods specified by the Vulnerability Threat Management Process.

For more information on the Vulnerability and Threat Management organization, see the following documents in particular.

[Vulnerability and Threat Management Life Cycle Process](#), Version 3.3.2.

[Product Alert List Maintenance Process](#), Version 2.1, September 30, 2004.

7.2.5 COB/Testing Schedule(s)

The COB plan and COB testing procedures are described in the SAN [COB PCM](#).

If you need help with LDRPS - access request, adjustments to user access profiles, plan tree adjustments (which include: Adds, Deletes, Moves and Copies), Inquiries and how-to questions; send an e-mail to: [LDRPS Admin Support](#).

7.2.6 Availability

The McData switch is operational 24x7. It is configured in a redundancy-networked topology.

7.3 EMERGENCY PROCEDURES/TROUBLESHOOTING

Emergency and troubleshooting procedures, such as problem ticket creation, assessing the severity, escalations, and notifications, are described in Section 3.2 of the [SAN-Problem Management PCM](#).

7.3.1 Level 1/2/3 support

Level 1/2/3 support and procedures, such as identification, ticket creation, severity level escalation, and determination, are described in Section 3.2.2 of the [SAN-Problem Management PCM](#).

7.4 LEVEL III PROCEDURES

At a minimum, the Level III procedures should include the following.

7.4.1 Audit Trail Review and Reconciliation

Audit trail review and reconciliation procedures, such as log reviews, are described in Sections 3.2, 5.2, and 5.3 of the [SAN-Information Security PCM](#).

7.4.2 Entitlement Reviews

Review procedures for entitlements, such as logging onto the server, launching the application, and navigating the menus, are described in Section 3.5 of the [SAN-Information Security PCM](#).

7.4.3 Security Incident Response

Security incident response procedures, such as auditing, logging attempted security violations, and significant events, are described in Section 5 of the [SAN-Information Security PCM](#).

7.4.4 Account Management

Account management procedures, such as access rights and employee status, are described in section 3.6 of the [SAN-Information Security PCM](#).

7.4.5 Data Backup and Retrieval

Data backup and retrieval procedures are described in the [SAN COB PCM](#).

If you need help with LDRPS - access request, adjustments to user access profiles, plan tree adjustments (which include: Adds, Deletes, Moves and Copies), Inquiries and how-to questions; send an e-mail to: [LDRPS Admin Support](#).

7.5 ASSET MANAGEMENT

Switch inventories are maintained within the [SAN-Resource Management PCM](#) asset-management documentation.

8 SUPPORTING DOCUMENTATION / REFERENCES

8.1 ADMINISTRATIVE GUIDES

8.1.1 Security Administration

Document Author:	Parul Jain
Author Org Type:	Distributed Storage Engineering
Author Phone Number:	212-816-4106
Author Email Address:	Parul.k.jain@citigroup.com
Author Department Name:	Distributed Storage Engineering
Document Location:	http://gdse.ny.ssmb.com/GDSE_docs/GDSE-03038-SG.pdf

8.1.2 System Administration

Document Author:	Parul Jain
Author Org Type:	Distributed Storage Engineering
Author Phone Number:	212-816-4106
Author Email Address:	Parul.k.jain@citigroup.com
Author Department Name:	Distributed Storage Engineering
Document Location:	http://san.ny.ssmb.com/GDSE_docs/GDSE-03038-SG.pdf

8.1.3 Operational Support Guide

Document Title	Author Info (name/organization)	Contact Info
SAN-Change Management PCM	Citigroup	Manuel Pantoja1-702-797-4448 manuel.pantoja@citigroup.com
SAN-Information Security PCM	Citigroup	Manuel Pantoja1-702-797-4448 manuel.pantoja@citigroup.com
SAN-Resource Management PCM	Citigroup	Manuel Pantoja1-702-797-4448 manuel.pantoja@citigroup.com

8.1.4 Help Desk / Emergency Procedures

Document Title	Author Info (name/organization)	Contact Info
SAN-Problem Management PCM	Citigroup	Manuel Pantoja1-702-797-4448 manuel.pantoja@citigroup.com

8.2 USER GUIDES

Document Author:	EMC CORPORATION
Author Org Type:	N/A
Author Phone Number:	N/A
Author Email Address:	N/A
Author Department Name:	N/A
Document Location:	http://powerlink.emc.com (Note: This site requires a login ID. For access, contact GSMG management.)

8.2.1 User Rights / Privileges

Document Author:	Parul Jain
Author Org Type:	Distributed Storage Engineering
Author Phone Number:	212-816-4106
Author Email Address:	Parul.k.jain@citigroup.com
Author Department Name:	Distributed Storage Engineering
Document Location:	http://gdse.ny.ssmb.com/GDSE_docs/GDSE-03038-SG.pdf

8.3 VENDOR DOCUMENTATION

Document Author:	EMC Corporation
Author Org Type:	N/A
Author Phone Number:	N/A
Author Email Address:	N/A

Author Department Name:	N/A
Document Location:	http://powerlink.emc.com (Note: This site requires a login ID. For access, contact GSMG management.)

8.4 INDUSTRY STANDARDS

Document Author:	EMC Corporation
Author Org Type:	N/A
Author Phone Number:	N/A
Author Email Address:	N/A
Author Department Name:	N/A
Document Location:	http://powerlink.emc.com (Note: This site requires a login ID. For access, contact GSMG management.)

8.5 SELF ASSESSMENT GUIDE

We use product and procedure TRAMS only. There are no self-assessment guides.

8.6 SAMPLE AUDIT LOGS

Symmetrix Array Logs

Sample output from the **symaudit -sid <sid> list -v** command:

Record Number : 309

Records in Seq : 2

Offset in Seq : 2

Time : 03/26/04 10:29:03

Vendor ID : EMC Corp

Application ID : ECC

Application Version : 5.1.0.0

API Library : SEK

API Version : V5.4.0.0 (Edit Level: 532)

Host Name : ECCTEST03AS

OS Name : WinNT

OS Revision : 5.0.2195Se

Client Host :

Process ID : 00001832

Task ID : 00002584

Function Class : DEVMask

Action Code : Add
Text : [0031 0091 0099]
Record Number : 310
Records in Seq : 2
Offset in Seq : 1
Time : 03/26/04 10:29:07
Vendor ID : EMC Corp
Application ID : ECC
Application Version : 5.1.0.0
API Library : SEK
API Version : V5.4.0.0 (Edit Level: 532)
Host Name : ECCTEST03AS
OS Name : WinNT
OS Revision : 5.0.2195Se
Client Host :
Process ID : 00001832
Task ID : 00002584
Function Class : DEVMask
Action Code : Add
Text : Added the following devices to the device masking data
base for Symmetrix 000387430127 by WWN 200000e069c01490 for director 35
for port 0

APPENDIX A: DOCUMENT REVISION HISTORY

Version	Change (Topic, section, page)	Author	Author Contact Information	Date
0.1	First draft	Vivek Jain	Vivek Jain	12/04
0.2	Sec 2.4, 6.5, 8.6	Vivek Jain	908-563-0019	02/05
0.3	Edit all hyperlinks to GSMG Level 3 PCM's and Sec.1, 1.1.3,	Gerald Walker	Gerald Walker 212-723-4756	04/05
0.4	Edit Sec. 1.1.7,2.1.1,2.1.3,	Gerald Walker	Gerald Walker 212-723-4756	04/05
0.5	Edit Sec. 2.4,3.5,6.2.1,6.2.3	Gerald Walker	Gerald Walker 212-723-4756	04/05
0.6	Edit Sec. 6.3.2.1,6.4.3	Bill Smith, Gerald Walker	Gerald Walker 212-723-4756	04/05
0.7	Edit Sec. 6.6.1,6.6.1.1	Bill Smith Gerald Walker	Gerald Walker 212-723-4756	04/05
0.8	Edit Sec.6.2.1, 6.2.3, (6.4.2 info-sec, baseline link)	Gerald Walker	Gerald Walker 212-723-7456	04/05
0.9	Edit Sec. 6.2.1	Gerald Walker	Gerald Walker 212-723-4756	04/05
0.10	Edit Sec. 6.2.3	Gerald Walker	Gerald Walker 212-723-4756	04/05
0.11	Edit Sec. 1.4 PCM definition	Gerald Walker	Gerald Walker 212-723-4756	05/05
0.12	Edit sec. 2.1.3,6.2.1,	Gerald Walker	Gerald Walker 212-723-4756	05/05
0.13	Updates from CSB certification	Vivek Jain		08/02/05
0.14	Updated to reflect addition of new DMX-3 model	Ludwig Derodel	Ludwig Derodel 631-712-7410	08/16/06

APPENDIX B: STANDARD AUDIT PROGRAM (SAP) / TAILORED REVIEW PROGRAM (TRP)

APPENDIX C: VULNERABILITY ASSESSMENT REPORT