

# Information Storage Security Design

## Course Description



### Course Number

MR-1CP-SECDSSW

### Delivery Method

Online Instructor-Led

### Duration

5 Days



This course material supports the EMC Proven Professional Program



EMC Corporation  
 Hopkinton  
 Massachusetts  
 01748-9103  
 1-508-435-1000  
 In North America  
 1-866-464-7381

EMC<sup>2</sup>, EMC, and where information lives are registered trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

© Copyright 2009 EMC Corporation. All rights reserved. Published in the USA.  
 1/06

EMC Education Services

*Last modified November 29, 2010*

### Overview

This course builds knowledge and skills required to successfully architect, design, implement, monitor, and maintain information storage security solutions to meet the needs of a business. It details a comprehensive, holistic, process-based approach that integrates business and technical factors to consider in the design of information storage security solutions to enhance their acceptability and business value. The course encompasses business strategy and its key criteria and perspectives, regulatory compliance, technical criteria, best practices, organizational structure, processes, people skills, and security posture. Included is a discussion of information security challenges and solutions in virtualized and cloud environments. Workshop style case studies at each design stage provide participants with an opportunity to apply their learning to real world situations.

### Audience

This course is intended for:

- Experienced IT professionals who are responsible for architecting secure information storage solutions
- IT professionals who have foundational knowledge on storage technologies and want to build their career in the storage industry
- Individuals who are seeking the EMC Proven Professional Data Center Architect (EMCDCA) Information Storage Security Specialist Certification
- Experienced security professionals with a basic knowledge of storage technologies (such as SAN and NAS) may also derive benefits.

### Prerequisite Knowledge/Skills

To understand the content and successfully complete this course, the student must have:

- An EMC Information Storage Associate (EMCISA) Certification
- A combination of knowledge and experience in computer networking and security that is equivalent to CompTIA's Network+ and Security+ curricula.

# Information Storage Security Design

## Course Description



**Course Number**  
MR-1CP-SECDSSW

**Delivery Method**  
Online Instructor-Led

**Duration**  
5 Days



This course material supports the  
EMC Proven Professional Program



EMC Corporation  
Hopkinton  
Massachusetts  
01748-9103  
1-508-435-1000  
In North America  
1-866-464-7381

EMC<sup>2</sup>, EMC, and where information lives  
are registered trademarks of EMC  
Corporation. All other trademarks used  
herein are the property of their  
respective owners.

© Copyright 2009 EMC Corporation. All  
rights reserved. Published in the USA.  
1/06

EMC Education Services

*Last modified November 29, 2010*

### Course Objectives

Upon successful completion of this course, participants should be able to:

- Identify various regulations, legislation and standards that affect a customer's information infrastructure and the customer's security issues
- Explain the role of an enterprise security policy and the critical components of that policy.
- Describe the importance of a security development lifecycle on the creation of secure products and the effect on operational security
- Explain how Security Configuration guides can be used to understand an organization's security problems
- Articulate the critical design decisions that support a secure storage environment
- List various implementation strategies for securely integrating storage products into a storage ecosystem.
- Explain the role of information storage security within virtualized environments
- Articulate how to maximize information storage security in Cloud computing
- Describe the role of secure logging in security auditing and SIEM
- Define vulnerability management and the process of reporting weaknesses
- List the key areas of data loss prevention
- List common characteristics of digital forensics when working with storage subsystems
- And thereby be able to hold credible conversations with other security personnel concerning storage products and technology
- All of these topics will be illustrated by EMC products, practices and services.

### Modules

Modules are designed to support the course objectives. The following modules are included in this course:

Module 0 – Course Introduction

#### Section 1: Building a Business Strategy for Storage Security

Establishes the business justification for storage security as a separate area of focus, explains how enterprise security policies must reflect the regulatory and legislative requirements, and details how various governance frameworks serve to support the ongoing design of secure storage solutions, coupled with the creation of specific storage security policies.

Module 01 - Motivating Storage Security

Module 02 – Regulations and Legislation

Module 03 – Governance Frameworks

Module 04 – Storage Security Policies

# Information Storage Security Design

## Course Description



**Course Number**  
MR-1CP-SECDSSW

**Delivery Method**  
Online Instructor-Led

**Duration**  
5 Days



This course material supports the  
EMC Proven Professional Program



EMC Corporation  
Hopkinton  
Massachusetts  
01748-9103  
1-508-435-1000  
In North America  
1-866-464-7381

EMC<sup>2</sup>, EMC, and where information lives  
are registered trademarks of EMC  
Corporation. All other trademarks used  
herein are the property of their  
respective owners.

© Copyright 2009 EMC Corporation. All  
rights reserved. Published in the USA.  
1/06

EMC Education Services

*Last modified November 29, 2010*

### Section 2: Choosing Secured Products

Addresses the need for procuring secured products by demonstrating how organizations can build security into their products, and illustrates how security deployment guides provide information to the system designer and the attacker as well.

Module 05 – Building Security In

Module 06 – Leveraging Deployment Guides

### Section 3: Designing for Secure Solutions

Covers the design and implementation process for providing secured storage solutions and discusses the particular requirements for securing storage in virtualized and cloud environments.

Module 07 – Design Considerations

Module 08 – Implementation Considerations

Module 09 – Securing Storage in Virtualized Environments

Module 10 – Securing Storage in the Cloud

### Section 4: Monitoring and Management

Addresses issues of monitoring, management and evaluation, covers how Security Information and Event Management (SIEM) and Data Loss Prevention (DLP) software systems provide evidence of regulatory compliance as well as indications of possible security incidents, and discusses Vulnerability Management and Digital Investigations to demonstrate both pro-active and re-active actions meant to ensure an organization's security posture, with examples taken from traditional SANs and virtualized and cloud environments.

Module 11 – Security Auditing and SIEM

Module 12 – Vulnerability Management

Module 13 – Data Loss Prevention

Module 14 – Digital Investigations in the SAN

Module 15 – Wrap-Up

# Information Storage Security Design

## Course Description

**Course Number**

MR-1CP-SECDSSW

**Delivery Method**

Online Instructor-Led

**Duration**

5 Days

**Case Studies**

Case studies reinforce the information that a student has been taught. In the case studies for this course, participants will work in teams on different technical cases set in different industries with different security challenges. Each case has the following phases.

Phase 0: Identifying an organization's critical information and infrastructure

Phase 1: Evaluating the security posture of the organization

Phase 2: Mapping security feature/functions to data storage security best practices and the organization's security policy

Phase 3: Responding to an organization's security concerns after installation

**Assessment**

Assessments validate that you have learned the knowledge or skills presented during a learning experience. This course includes an assessment upon conclusion.



This course material supports the  
EMC Proven Professional Program



EMC Corporation  
Hopkinton  
Massachusetts  
01748-9103  
1-508-435-1000  
In North America  
1-866-464-7381

EMC<sup>2</sup>, EMC, and where information lives  
are registered trademarks of EMC  
Corporation. All other trademarks used  
herein are the property of their  
respective owners.

© Copyright 2009 EMC Corporation. All  
rights reserved. Published in the USA.  
1/06

EMC Education Services

*Last modified November 29, 2010*