

Realtime  
publishers

"Leading the Conversation"

# *Tips and Tricks Guide™ To*

# Creating Business Continuity through Enterprise Storage Solutions



*Chad Marshall*

**Note to Reader:** This book presents tips and tricks for seven topics related to business continuity created through enterprise storage solutions. For ease of use, the questions and their solutions are divided into topics, and each question is numbered based on the topic, including

- Topic 1: Securing Availability and Business Continuity
- Topic 2: Maximizing Storage Resources and Solutions
- Topic 3: Information Management
- Topic 4: Cost Management
- Topic 5: Compliance
- Topic 6: Security
- Topic 7: Aligning Storage to Serve Business

Topic 6: Security.....	1
Q6.1: What is storage resource management and how can it enable tighter security controls in enterprise storage? .....	1
The Role of SRM in Security.....	2
Q6.2: What are the best practices for enterprise storage security? .....	3
Policies.....	3
Confidentiality .....	4
Integrity.....	4
Availability .....	4
Standards.....	4
Guidelines .....	4
Procedures and Practices.....	4
Baselines .....	4
Best Practice 1: Obtain Senior Management “Buy-In” .....	5
Best Practice 2: Develop and Implement Storage Standards.....	5
Best Practice 3: Ensure Patch Levels and Unit Acceptance Testing .....	6
Best Practice 4: Actively Develop, Apply, Challenge, and Tweak Baselines.....	6
Best Practice 5: Use Only Proven Technology.....	6
Best Practice 6: Audit Often .....	6
Best Practice 7: Educate, Educate, Educate.....	7
Best Practice 8: Don’t Go it Alone .....	7
Q6.3: What steps can be taken to ensure the physical security of data?.....	8
Secure Facility .....	8

Physical Location and External Layout .....8

Building Engineering and Internal Layout .....9

Access Control .....9

Bringing It All Together .....10

Q6.4: What is the role of data encryption in storage management? .....10

    Encryption on Media.....11

    Encryption During Transfer .....11

Q6.5: What are the best identity and access management strategies to secure my company’s data? .....12

    Best Practice 1: Obtain Senior Management “Buy-In” .....12

    Best Practice 2: Don’t Try to Boil the Ocean .....12

    Best Practice 3: Identify Complacency and Systematically Eliminate It .....13

    Best Practice 4: Implement Multiple and Mutual Factor Authentication .....13

    Best Practice 5: The Best Security System Is an Alert Associate.....14

Q6.6: What is the role of security management in regulatory compliance?.....15

    Identity Management, Provisioning, and Access Management.....15

    Monitoring .....15

    Auditing .....15

Q6.7: What specific security requirements must be adhered to when dealing with United States government records?.....16

Download Additional eBooks from Realtime Nexus! .....17

## Copyright Statement

© 2007 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at [info@realtimedpublishers.com](mailto:info@realtimedpublishers.com).

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

## **Topic 6: Security**

### **Q6.1: What is storage resource management and how can it enable tighter security controls in enterprise storage?**

**A:** Storage resource management (SRM) is the management of physical and logical storage resources, including storage devices, appliances, virtual devices, disk volumes, and file resources. What this typically relates to in practice is management designed to ensure that the right storage solution, in terms of cost and performance, is properly aligned to the business need.

For example, if a storage resource is being requested to meet the needs of a production database accessed by thousands of users per day, it can be generally assumed that the storage resource is going to need to be capable of high-performance input and output (I/O). Conversely, if a storage resource is being requested for a document management archive that may only be accessed by a handful of users per month, a lower-performing, and thus less expensive, solution may be aligned. Identifying what criteria a given application system requires equates to a “right sizing” of the environment. While back-end routines for SRM are often focused on identifying misaligned storage resources, the front end, in a consultative approach, should be focused on asking the right questions. The efficiency of the SRM process will usually have a direct financial impact as business needs are understood the cost over-runs associated with overbuying can be avoided.

SRM can be further defined in its added capabilities of providing a consolidated view of storage resources and offering the capability to monitor and measure storage status across the enterprise. Deploying active management alternatives to prevent interruption of service is just one benefit of SRM. Through effective management routines, SRM can also be used as a tool to ensure that adequate plans are in place to forecast future growth.

An effective SRM system should be able to:

- Provide an “Executive View” of storage network health showing what resources are available enterprise-wide, how they’re being used, and how they are related.
- Provide for simplified monitoring and management of networked storage resources and applications for improved operational efficiency and helping you avoid over-provisioning resources while others are underused. This reduces the expense of additional storage devices that might not really be needed.

- Provide trend analysis that monitors how much new content is being added to storage on a regular basis and identify which consumers are using the most capacity. With this information, you can plan for the future effectively and anticipate your needs before a crisis occurs.
- Have the ability to provide centralized reporting and monitoring of multi-vendor backup and recovery applications, which can increase operational efficiency and mitigate the risk of data loss and mismanagement.
- Be able to automate essential storage processes. This can improve overall human resource efficiency by minimizing time spent managing the storage environment, performing tasks such as configuring storage area network (SAN) components, moving data from one storage device to another, and provisioning new storage space.

### ***The Role of SRM in Security***

Security is about more than just limiting access; it's also about ensuring that those who have a need to access the information are granted that capability. The administration of security controls is centered on processes that are primarily concerned with implementing and managing security controls to meet corporate security policies. The goal of those processes is often to ensure that systems security, and subsequently the data managed by those systems, meets confidentiality, integrity, and availability requirements. SRM and security directly relate to each other insofar as data must always be aligned to a properly restrictive storage resource.

When data exists on a direct attached storage (DAS) device, that data can be controlled rather granularly through the security architecture of the operating system (OS) by using usernames and passwords or other forms of access control. However, when data is moved out from underneath the direct control of a single OS or domain-controlled access list, such as when it is stored on tape, then a great deal of security control can be lost. Understanding where security control aligns with your various security resource offerings and working closely with information security partners to define new alignments to meet business needs is an important part of SRM.

In addition to leveraging SRM to properly align security controls to storage resources, an effective SRM process will enable line of business and application managers to understand, measure, reduce, and mitigate operational and business risk by identifying areas of storage resource misalignment. Doing so will enable those business partners to achieve their organization's goals of ensuring ongoing service continuity and ensuring compliance with regulations. It will also enable broader visibility of security resource utilization back to the consumers, which, aside from the obvious benefit of financial transparency, will increase awareness of how storage resources are being consumed (and by whom). This can simplify security management by bringing attention to clear areas of resource utilization that may not directly surface through any other processes in such a neatly packaged format.

## Q6.2: What are the best practices for enterprise storage security?

**A:** Storage security starts with a solid foundation of best practices that include the development of a framework of policies, standards, guidelines, procedures and baselines that clearly document, provide focus, and deliver guidance at all levels of an organization.

### **Policies**

When examining what it is that makes an enterprise storage infrastructure secure, you must start at the highest level of an organization and begin with the development and implementation of a sound storage security policy. A policy is a framework within which an organization establishes levels of information security to achieve the desired confidentiality, integrity, and availability goals. A policy is essentially a statement of information values, protection responsibilities, and organization commitment for a system.

A soundly designed and implemented storage security policy is vital to the confidentiality, integrity, and availability of any storage environment. These three components form what is known in information security as the C-I-A triad.



**Figure 6.1: The CIA triad.**

## **Confidentiality**

Confidentiality is a concept centered on the prevention of unauthorized disclosure of data. Disclosure of data through the loss of confidentiality can occur in any number of ways including deliberate release, inaccurate or ineffective security controls, or the failure to apply properly defined security controls.

## **Integrity**

Integrity is a concept that focuses on ensuring that no unauthorized alterations are made to data. Integrity loss can occur through any number of ways including deliberate unauthorized tampering, software or hardware malfunction, and human error.

## **Availability**

The concept of availability is one that focuses on timely delivery of data to those who require access; that is to say, ensuring all who need access receives access when they require it. Loss of availability, like integrity, can result through deliberate action, unauthorized use or misuse, software or hardware malfunction, and human error.

Maintaining confidentiality, integrity, and availability is essential to enterprise and storage security.

## **Standards**

A standard is a document that defines the specific use of technology and the manner in which it is used. The implementation of standards within an organization provides for uniformity throughout the enterprise. For example, your organization may have recognized the use of a specific kind of SAN architecture as a standard to provide for uniformity of SAN storage architecture throughout your organization.

## **Guidelines**

A guideline is similar to a standard in that they both specify the use of technology; however, unlike standards, guidelines are merely recommendations that should be followed. An organization is likely to have many standards but few guidelines.

## **Procedures and Practices**

A procedure (or practice) is a detailed process flow for performing specific tasks within the organization.

## **Baselines**

Baselines are the minimum acceptable security that should be provided to protect information resources and are usually delivered at the platform level. For example, a SAN solution that is being delivered specifically in support of a public-facing document repository may have a baseline of security controls that must be met that covers how the device is to be installed, configured, accessed, managed, and administrated. A storage security policy is one piece of a larger security policy hierarchy that begins with a statement of policy by senior management, as Figure 6.2 illustrates.



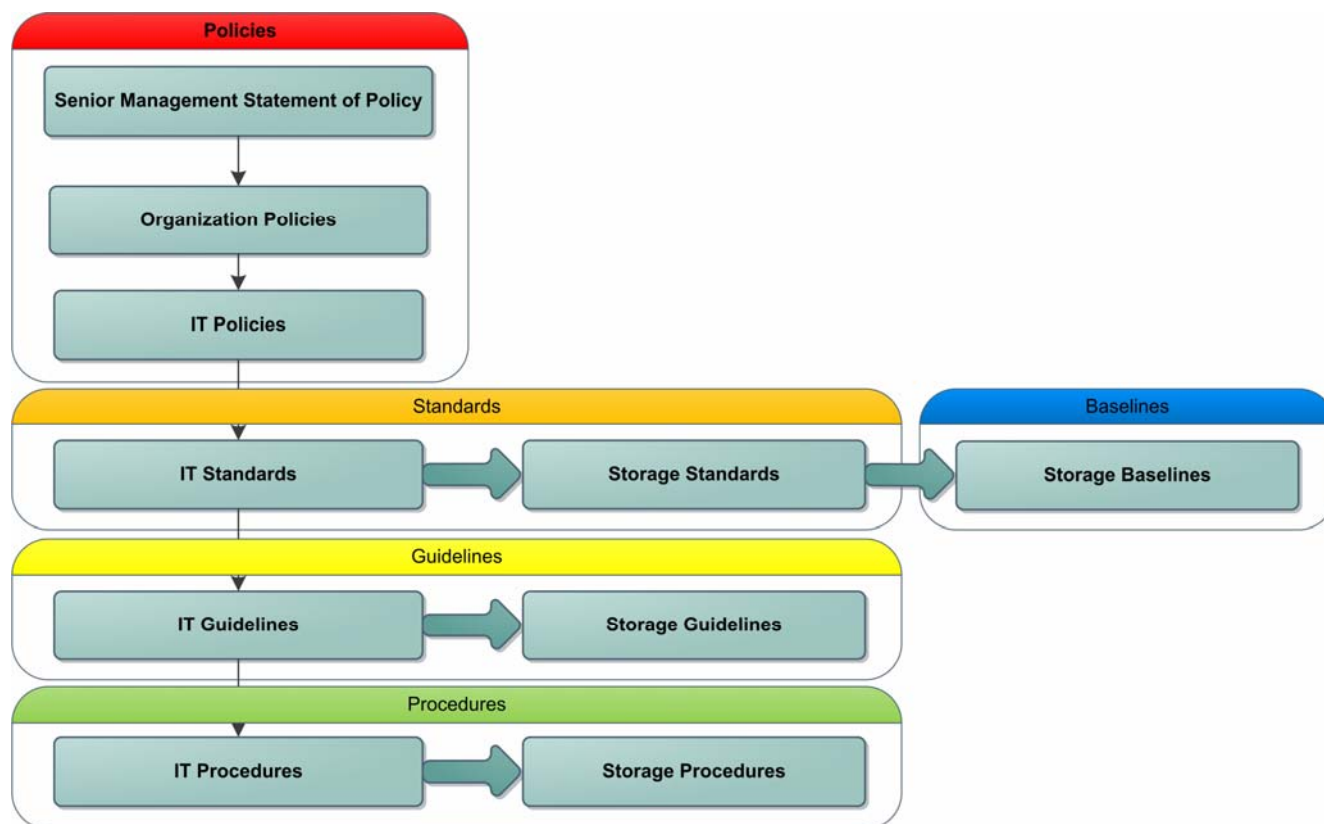


Figure 6.2: Policy hierarchy.

### **Best Practice 1: Obtain Senior Management “Buy-In”**

The first step in achieving enterprise storage security is obtaining the full support of senior management through the development of a senior management statement of policy. This policy should be a simple and straight-to-the-point message that acknowledges the need of information systems security policies, declares support for information systems security, and sets forth a commitment by senior management to authorize and manage the creation of lower-level policies.

### **Best Practice 2: Develop and Implement Storage Standards**

Once you have the support of senior management, work with your information security partners to develop and implement standards, guidelines, procedures, and baselines the purpose of which is to protect the storage network and aide in maintaining the confidentiality, integrity, and availability of data. These documents will cover a broad range of IT needs. In terms of storage security, be particularly concerned about both data residing on storage media and data traveling through the network. These policies should also address how storage is backed up, restored, monitored, and audited. Whenever possible, policies, standards, and guidelines should overlap to reinforce each other and provide multiple layers of security.

**Best Practice 3: Ensure Patch Levels and Unit Acceptance Testing**

All storage systems should be upgraded as new software releases, security hot fixes, or firmware upgrades become available and are tested in a Unit Acceptance Testing environment. A UAT environment helps to ensure that software or firmware upgrades are tested prior to being deployed to a production environment by first deploying the upgrade to a device specifically set aside for such testing. The UAT environment should always be an *exact copy* of the production environment whose use is solely that of UAT testing and *should not* be used for any other testing or development work. This is to ensure that when a zero-day vulnerability (meaning a vulnerability for which a known exploit currently exists) is discovered, your organization can test immediately without interrupting any other testing schedule or development work.

**Best Practice 4: Actively Develop, Apply, Challenge, and Tweak Baselines**

This process is known as system hardening. Out of the box, most systems are woefully insecure and provide scarcely enough documentation to keep even the most insincere of hackers at bay. Hardening is the process of securing a system and usually involves the removal of unnecessary access rights, the disabling or complete removal of unnecessary services or daemons, installation of patches, and the configuration of baseline security settings. Hardening of an environment (beyond just a single system or storage device) may also include the installation and configuration of firewalls, intrusion detection systems, and intrusion prevention solutions.

**Best Practice 5: Use Only Proven Technology**

Ask anyone who purchased a “Betamax” video recorder and they will attest that superior quality does not always equal a superior product in the marketplace. Make sure that your procurement practices align to ensure that only proven technologies are installed in your storage environment. Each new, or emerging, technology should be vehemently researched for compatibility of architecture and alignment to current standards and baselines.

**Best Practice 6: Audit Often**

Most IT professionals will agree that an actual audit is the second-to-worst possible time to discover an audit failure—preceded only by an actual attack—and both may, depending upon the size and scope of the violation, be career-altering events. The unfortunate perception, however, is that auditing is a self-serving activity much like “housekeeping” work and is often underemphasized. Take steps to emphasize it. This may include incorporating regular system log reviews into a daily routine. If your organization maintains an on-call rotation of storage engineers, a good practice is to assign the engineer who is next to come on rotation the job of reviewing logs so that when they start their rotation they will have a clear perspective of any security events that may have recently occurred.

**Best Practice 7: Educate, Educate, Educate**

Education is a powerful yet often underutilized tool. Many organizations struggle just to maintain the mandatory training programs relating to sexual harassment or insider training and rarely dedicate time to educating on security essentials or developing conduits for their associates to maintain awareness of security issues and how they may impact the organization. Regular education and training combined with tools to maintain situational awareness are vital to maintaining a secure storage infrastructure. Education and training can be classified into these three areas:

- **Organizational (mandatory) Training**—At the highest level of the organizational education spectrum is organizational training. This training is usually mandatory and covers a broad area of topics. If an information security training program has not yet been mandated at this level, it should be. Consult with your information security department to educate users through organizational training on security topics relating to storage security, such as data classification. Using this time to put in a quick “bullet” as to why users are not allowed to store .EXE files on their shared drive, for example, may eliminate a few calls to your storage team by users so inclined to attempt to do so.
- **Job Specific**—Like everything else in IT, storage technologies change rapidly. Lowering costs of physical media has driven many new, diverse, and often competing technologies. A job-specific training program should be developed in conjunction with storage standards for your organization to ensure that all storage (and other IT personnel) have access to the training they need to fully utilize the storage infrastructure. One way to do so might be to develop a “Storage Engineering Playbook” that covers all the major areas of storage architecture and provides direction on where to go to learn more about a particular storage product or service offering.
- **Situational Awareness**—New technologies are being developed nearly every day. Service packs, hotfixes, application updates, and firmware upgrades can be deployed at any time, day or night. How do we keep track of it all? In addition to subscribing to any of more than a dozen periodicals on enterprise storage to maintain an industry perspective, another way is to use an alerting service.

**Best Practice 8: Don't Go it Alone**

IT professionals have an advantage that line of business professionals often lack and that is (unless you work in R&D) that you can, for the most part, openly converse with outside colleagues about topics concerning your infrastructure woes. Although the folks in marketing might get in trouble for discussing the details of a new campaign, IT staff is relatively free to discuss the storage infrastructure, ask opinions, get advice, and share what you know so long as you keep the conversation focused on the technology (and not the specific data). This is a tremendous leveraging tool that enables the pooling of outside resources.

### Q6.3: What steps can be taken to ensure the physical security of data?

**A:** Physical security is a security discipline focused on the prevention and or determent of attackers from accessing a facility, resource, or information stored on physical media. Implementing physical security controls can be as simple as securing a drawer, file cabinet, or door with a lock or as complex as multiple roving armed guards and a 1000-camera closed-circuit facility monitoring system. Ensuring physical security requires a holistic view of how data is handled and where it's handled. As the concept of the data center is central to many organizations, let's begin with a focus on securing the data center.

#### **Secure Facility**

Designing a secure data center is the first stage in ensuring the physical security of data. The United States government provides several guidelines for building a secure structure, and guidance is also available from public sector groups such as the National Fire Protection Association. At a high level, you're essentially going to need to be focused on three key areas:

- Physical location and external layout
- Building engineering and internal layout
- Access control

#### **Physical Location and External Layout**

Ensure that the data center is in a secure location preferably far away from your main offices. Doing so will ensure that any impact to the main office facility won't wipe out your entire operations. The building should also be a considerable distance from heavily trafficked roads, at least 250 meters away from traffic; this will help to ensure that any traffic accident that might occur near the premises won't involve the building itself. Choosing a location away from other potential threats or targets should also be a consideration. Government offices, airports, chemical plants, power plants, and water and other public utilities all may be at risk for a targeted act of terrorism. Further, airports, chemical plants, and power plants all hold the potential for an accident to occur that may impact your operations. Stay away from these neighbors.

Geographically, you'll want to consider a location that is away from all the major natural disaster-prone areas. The coastline, anywhere near moving water (think flooding), and areas near geographic faults should definitely be avoided. On the local geographic scale, the layout of the land on which the building is to be placed is also important. Using soil that was moved to construct the building to create an earthen wall is an inexpensive and practical means of making a natural wall around the property that will obscure public view, offer protection from unauthorized vehicle entry, and can be landscaped to enhance the outward appearance. If the local geography can't be leveraged, use crash-proof barriers in combination with fencing to restrict access. The goal should be to maintain at least 100-meter buffer zone around the immediate facility.

## Building Engineering and Internal Layout

When designing a data center, the focus must always be on protecting the data. Therefore, your data center is likely to have more characteristics of a vault than an office building. Thick concrete walls to provide protection from storms, natural disasters, fire, and acts of terrorism should be used throughout the facility. Keep windows to a minimum. Wherever windows must be used, be certain to use bomb-resistant glass.

Protection for the building heating, air-conditioning, power distribution, and utilities should be designed with the same rigid access controls given to the data itself. Unauthorized access to a power distribution panel, for example, could bring down the entire facility and access to an air-condition system could easily allow someone to introduce a chemical or biological substance that would impact the entire facility. Make sure that power equipment, such as generators, are located away from any potential flooding hazard and that environmental systems are tamper proof. For added protection, chemical, biological, and radiological sensors should be considered.

## Access Control

Controlling access to the facility is of paramount concern, so whenever possible, use at least two-factor authentication. There are three universally recognized factors for authenticating individuals:

- Something you know, such as a password
- Something you have, such as an issued identification badge or hardware security token
- Something you are, such as a fingerprint, a retinal scan, or other biometric

At least two of these three should be required to gain access to the building. For example, an employee entering the data center may be required to enter a personal identification number (PIN—something they know) at the door and swipe their ID badge's magnetic strip through an access device to gain entry. The number of entry points should also be limited to control access to the building. Guards positioned at each entry point should be empowered to challenge any suspicious person, demand proper identification, and perform random searches of all who enter or leave the premises.

Exit points for the building should be as many as are required by local regulations, but all exit-only points should be triggered with an alarm. You may also consider removing the handles on the outside of exit-only doors to prevent attempts at unauthorized access. Internal passageway points should be designed with fire containment in mind. Fire doors may be held open with magnetic plates that disengage when the fire suppression system is engaged; this will help limit the spread of a fire and not only serves to protect against loss of life but also may give the fire department a few more moments to arrive onsite to combat the blaze.

Closed Circuit Television (CCTV) cameras should be used widely throughout the building to monitor all potential entry and exit points. Digital Video Recorders (DVRs) allow for surveillance footage to be transmitted offsite, so you may consider leveraging the existing network infrastructure to allow for surveillance video to be stored in a remote location. Using a combination of both overt and covert camera placements will help to ensure maximum coverage without pointing out any potential targets. For example, if the building generator is located behind a concrete wall outside the back of the building, placing an overt camera may draw attention to its location; instead consider using a covert camera to monitor the location without giving away the equipment's location.

### **Bringing It All Together**

The physical location, external layout, building design, internal layout, and access controls should all come together to build layers of security control with the least-restrictive access controls on the perimeter. The more restrictive access controls being enforced, the closer a person gets to the actual data. By the time any person gets hands on access to the data, they should have been through at least three checkpoints; one at the perimeter of the property, a second at the point of entry, and then again at a third as they enter the actual data center portion of the building. Their image should have been captured via CCTV at all three checkpoints, with detail enhancing the closer they get to the data, and their entry acknowledged or witnessed by at least one security guard to provide an actual human element to the equation. To further augment the human element and limit the predictability of security measures, roving guards should be deployed at random intervals and times with non-specific and non-published routes.

### **Q6.4: What is the role of data encryption in storage management?**

**A:** Protecting the confidentiality, integrity, and availability of data is the hallmark of information security, and with regulatory and compliance concerns on the rise, these tenants of information security are on the top of many IT executives minds. Recent losses of tape media by several major corporations and government agencies have illustrated the need to secure data well beyond the physical control of the media. Encryption, which is the process of obscuring information to make it unreadable without special knowledge, contributes to information security by obscuring data. Whether the data is contained on storage media or being transferred on a storage area network (SAN) to end users, encryption technologies are becoming an integral part of storage management to protect data from unauthorized disclosure.

### ***Encryption on Media***

In April 2005, Ameritrade Financial warned approximately 200,000 customers of the loss of a backup tape containing their personal information. In June of the same year, Citigroup announced that personal information about 3.9 million consumer-lending customers of its CitiFinancial subsidiary was lost by UPS while in transit to a credit bureau. And in May of 2006, the U.S. Department of Veterans Affairs reported the loss of a laptop containing the sensitive personal information of 26.5 million veterans and military personnel. All of these cases involved the loss of physical control of media. Encryption helps to mitigate the risk of compromised data associated with lost media by obscuring the data and should be considered standard practice for any physical media that contains sensitive, confidential, or proprietary data. Tape backups over the years have been the most common form of compromised physical media either through employee negligence, vendor negligence, or intentional theft; technologies are now available that are both cost effective and easy to integrate and manage into the backup and recovery process.

When choosing an encryption product, partner with a reputable storage vendor that will help you select the proper encryption product for your environment. Not all media encryption products are the same nor do they use the same methodology, so be certain to choose one whose encryption methods encrypt data as it is being created as opposed to those that go back after the data has already been written to tape. This increases the security by preventing tools used in computer forensics being used to recover previously written data from the media.

### ***Encryption During Transfer***

In addition to being a mechanism to keep data safe as it travels outside of the organization on physical media, encrypting data as it travels through the storage infrastructure contributes to overall data security as well by obscures the data in transit. This helps to prevent hackers from eavesdropping on corporate networks and capturing data. One of the main advantages of storage encryption during transfer is that it protects the data at a relatively low cost. Multiple ciphers can be used for individual files, folders, or data volumes depending upon need and usage, which makes encryption “over the wire” a cost-effective goal.



## **Q6.5: What are the best identity and access management strategies to secure my company's data?**

**A:** Identity and access management have become increasingly complex. Organizations need to manage user identification access efficiently and accurately, ensuring that their employees are only granted access to the resources they are entitled. A major challenge in this area, however, is that identity and access management controls are rarely implemented universally. Through organization changes such as mergers and acquisitions, software upgrades, job and role changes, and changes in the identity and access management processes, the capability of many organizations to provide consistent and effective identity and access management has become degraded.

Turning this situation around is a daunting challenge for many organizations, but the business benefits are clear. By implementing a consistent identity and asset management strategy, an organization can reduce the total cost of ownership (TCO) of identity and access management through consolidation of systems. Further, improvements to identity and access management lower the potential risk of both internal and external attacks and make regulatory compliance challenges easier to meet; fewer access systems through consolidation equates to fewer audit points of failure. Developing a consistent and effective identity and access management strategy, however, will require a sound understanding of the approaches and technologies used to address multiple identities an employee may require to fulfill their role.

### ***Best Practice 1: Obtain Senior Management “Buy-In”***

As has already been stated within this guide, the first step in achieving security is obtaining the full support of senior management. Implementing an ID and access management strategy is often a self-funded enterprise initiative, so full support of senior management is going to be critical to securing and maintaining funding. Further, as ID and access management impacts every employee, senior management will also be important where changes in corporate culture are required.

### ***Best Practice 2: Don't Try to Boil the Ocean***

That is to say that you're likely not going to get everything in the entire realm of ID and access management under control with one large “super project.” The first step in developing a strategy will be to conduct a risk assessment designed to identify and prioritize areas of ID and access risk. Once your largest areas of risk are identified, begin tackling each discipline one-by-one. For example, if your organization's biggest ID and access risk involves multiple user accounts and passwords being used to access systems within the enterprise, focus on those systems that will mitigate the risk to the greatest possible degree. Implementing a single-sign-on (SSO) product may seem like a great way to connect multiple disparate access systems (and it is), but if your organization has 10 or more Windows domains to which users need to authenticate, you may be better served through a system consolidation effort first.



**Best Practice 3: Identify Complacency and Systematically Eliminate It**

All the best identification and access management products in the world are useless if employees do not respect identification and access policies. The first step in driving respect is the buy-in from senior management. The next is the development of a policy that ties directly to individual employee performance metrics. The third is to include employees in the development and implementation of access controls. It is very easy to spout security policies and rules when you're not the one directly impacted by the policies and rules. To end users, this often equates to corporate dogma and becomes viewed as obstacles to be circumvented rather than tools to reduce operational risk. Often you may find that employee frustrations when given time and consideration by IT managers will equate to financial savings. For example, employees performing a "production" role in an organization were once called upon to have to maintain three separate logons and passwords. The first was to log on to the production PC. The second was to log on to the production application, and the third was for a separate "non-production" computer used for corporate email and word processing. All three systems had different user naming conventions and password policies that required a unique username and password. Users became so frustrated from calling the Help desk to have their passwords reset, they began writing down their usernames and passwords and were prone to share their logon information with other employees in the interest of "productivity." This was clearly an opportunity for consolidation that would benefit not only the associate but also reduce risk by simplifying the ID and access management control structure.

**Best Practice 4: Implement Multiple and Mutual Factor Authentication**

In security management, a factor is a property an individual possesses that provides non-repudiation. As explored in Question 6.3, there are three universally recognized factors for authenticating individuals:

- Something you know, such as a password
- Something you have, such as an issued identification badge or hardware security token
- Something you are, such as a fingerprint, a retinal scan, or other biometric

Providing a personal identification number (PIN) along with your debit card is an example of two-factor authentication because it requires both something you know (your PIN number) and something you have (your debit card). In contrast, a system that requires both a username and a password is an example of a single-factor authentication because both items (username and password) rely on a single factor (something you know).

The most common form of identification is the first factor, "something you know," and many organizations stack layers of this identification method upon one another. Username and password being most commonly overused. This is due in no small part to it being the most inexpensive and easily implementable of all the factors of identification. Issuing ID badges or hardware tokens or implementing biometric technology all require some degree of capital expenditure.

It is also important to note that mutual authentication may serve as a secondary factor. This is especially useful in instances where only a single factor, such as “something you know” is available. Bank of America became an industry leader in online banking security by implementing what essentially is a mutual authentication system called SiteKey. Here’s how it works: After entering in a user account number online, customers are then given a response from the Web site in the form of a pre-selected image. If the user recognizes the image as the one they had pre-selected when setting up their online account, they may then choose to enter in their password to access online banking. The resulting factor roles play out like this:

- Online banking customer presents account number (something they know that Bank of America can validate)
- Online system responds with pre-selected image (something the online system knows that the user can validate)
- Online banking customer responds with password (something they know that Bank of America can validate)

This mutual authentication method then becomes a rather inexpensive means of augmenting what would otherwise remain a single-factor authentication environment.

### ***Best Practice 5: The Best Security System Is an Alert Associate***

Ask yourself this question: The last time you went on vacation, did you call the police and inform them that you would be out of town or did you ask your neighbor to keep an eye on your place? The best response would be both but the most likely response is that you asked a neighbor or someone else nearby, a friend or relative perhaps, to check in on your assets while you were away and chances are they agreed. Perhaps out of some degree of neighborly responsibility, or good citizenship, or maybe just out of their desire for you to do the same when they go out of town but no matter what the motivation it is a winning relationship. Why? Because your neighbor knows the neighborhood, they’re present and they are empowered by your request to do something about suspicious activity. Building a corporate culture that promotes security often simply requires that last step: empowering employees to do something about it. If anyone notices anything suspicious or out of the ordinary in the work place, they should be empowered to take action and feel that such conduct will be received as acceptable behavior. An employee being 5 minutes late to a meeting, for example, because he stopped to make sure two “strangers” were authorized to be on the floor should be considered acceptable behavior.

## Q6.6: What is the role of security management in regulatory compliance?

**A:** Security management plays a central and immutable contributing role to regulatory compliance. Within an organization, security management is responsible for ensuring regulatory compliance by designing and implementing security measures to meet the regulatory and compliance needs of the organization through identity and access management, provisioning, monitoring, and auditing.

### ***Identity Management, Provisioning, and Access Management***

Identity management, provisioning, and access management are the three most focused disciplines of security management. Identity management is focused on the management of data used to positively identify an individual beyond a reasonable doubt. Provisioning is the granting or denial of equipment or data needed to perform a function. Access management is the management of the capability of an individual to access a secure location or systems. This realm of security management spans from access to physical assets and facilities to electronic access to remote computer systems.

### ***Monitoring***

It is in the best interest of any organization to know when, where, and how their systems are being accessed at all times. In the physical security domain, monitoring may include a Closed Circuit Television (CCTV) system or alarm monitoring used to help ensure the physical security of the data is maintained. Within the network infrastructure, monitoring may include intrusion detection and intrusion prevention systems designed to detect, alert, and prevent unauthorized access to data. All forms of monitoring contribute to regulatory compliance by helping to ensure the physical security of the data.

### ***Auditing***


Security auditing is a systematic evaluation of security controls designed to measure how well an organization's controls meet established criteria. In the context of regulatory compliance, security auditing can be specifically designed to seek out and identify at-risk controls within an organization. Designing an audit specifically geared towards detecting an organization's ability to meet the requirements of the Sarbanes-Oxley Act, for example, is one significant role auditing can contribute to regulatory compliance.

Within the ever-changing landscape of security and regulatory compliance, the role of the security manager is made even more challenging by a need to keep security constraints aligned to business needs. Too loose a control and the organization risks financial losses through regulatory penalties; too restrictive a control and the organization may risk degradation in productivity that too equates to financial losses. Quantifying and managing these risks will be crucial to the success of security management.

## Q6.7: What specific security requirements must be adhered to when dealing with United States government records?

**A:** The United States government, like any bureaucracy, has layers upon layers of requirements that may need to be adhered to depending upon what, exactly, it is that needs to be accomplished and what government agency you're working with. A good resource within the U.S. federal government for identifying security requirements is the National Institute of Standards and Technology's Computer Security Division Computer Security Resource Center, also known as the NIST CSRC (<http://csrc.nist.gov/>). The Computer Security Division has a mission that includes developing standards, metrics, tests, and validation programs to promote, measure, and validate security in systems and services, educate consumers, and establish minimum security requirements for federal systems. This division is also responsible for developing guidance to increase secure IT planning, implementation, management, and operation.

Often of specific interest to storage and records management interacting with the U.S. government is DoD 5015.2. DoD 5015.2 is a records management certification managed by the Joint Interoperability Test Command of the United States Department of Defense (DoD). Under this article are two separate and distinct certifications—Chapter 2 and Chapter 4.

 Full details about DoD 5015.2 can be found on the Defense Information Systems Agency Web site at <http://jitc.fhu.disa.mil/recmgt/standards.html>.

And while the complete details of DoD 5015.2 are quite lengthy, the general requirements for records management applications (RMAs) are provided here to illustrate the major points of the requirements document.

### DoD 5015.2 General Requirements

**Managing Records.** RMAs shall manage records in accordance with this Standard, regardless of storage media or other characteristics (see 44 U.S.C. 3103 and 36 CFR 1222.10, references (p) and (q)).

**Accommodating Dates and Date Logic.** RMAs shall correctly accommodate and process information that contains dates in current, previous, and future centuries (see FIPS 4-2, reference (r)). The capability shall include, but not be limited to, century recognition, calculation, and logic that accommodates same century and multi-century formulas and date values, and date interface values that reflect the century. RMAs shall store years in a 4-digit format. Leap year calculations shall be accommodated (e.g., 1900 is not a leap year; 2000 is a leap year).

**Implementing Standard Data.** RMAs shall allow for the implementation of standardized data in accordance with DoD 8320.1-M (reference (s)). When selecting commercial-off-the-shelf (COTS) products to support RMA requirements, selection criteria should include the feasibility and capability of the COTS products to implement and maintain DoD data standards. This requirement implies the capability for adding user-defined metadata fields and modifying existing field labels.

**Backward Compatibility.** RMAs shall provide the capability to access information from their superseded repositories and databases. This capability shall support at least one previously verified version of backward compatibility.

**Accessibility.** The available documentation for RMAs shall include product information that describes features that address 36 CFR parts 1194.21 and 1194.31 (references (t) and (u)). For web-based applications, 36 CFR part 1194.22 (reference (v)) shall also apply (see 29 U.S.C. 794d, reference (w)).

If your organization intends to do work with the DoD, you'll need to familiarize yourself with this standard and ensure compliance.

## Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.