

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 5: Compliance.....1

Q5.1: How do compliance concerns influence storage, business continuity, and disaster recovery planning?.....1

Compliance Impact on Storage.....1

Compliance Impact on Business Continuity Planning and Disaster Recovery Planning ....2

Q5.2: In an environment of increasingly complicated regulatory and legislative compliance concerns, what steps can be taken to minimize the impact of these concerns on the storage infrastructure? .....3

Integrate Compliance Needs into Service and Operating Level Agreements.....3

Standardizing Product and Service Offerings.....3

Integrate Compliance in Information Life Cycle Management.....4

Q5.3: What major factors influence compliance today and how might they influence storage solutions tomorrow?.....4

Q5.4: How do SOX, GLBA, SEC 17A, NASD, HIPAA, and other U.S.-based compliance requirements specifically impact storage and information management?.....4

The Sarbanes-Oxley Act.....5

The Gramm-Leach-Bliley Act .....5

Securities Exchange Commission Rule 17A .....6

NASD.....8

The Health Insurance Portability and Accountability Act.....8

Q5.5: What steps can I take to ensure compliance in my environment? .....10

COSO .....10

COBIT.....11

Q5.6: How do international standards, such as the United States DoD 5015.2, ISO 15489, and MoREQ, effect storage and information management requirements and implementations? .....12

DoD 5015.2.....12

ISO 15489 .....13

MoREQ.....14

Q5.7: What best practices or guidelines exist that can help ensure corporate governance?.....15

    Build a Culture of Accountability.....15

    Emphasis Process over People.....15

    Identify Strategic Value .....16

    Set Clear Priorities .....16

    Audit Often .....16

---

## Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.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 Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.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.

Realtimepublishers.com and the Realtimepublishers 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 Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.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 5: Compliance**

### **Q5.1: How do compliance concerns influence storage, business continuity, and disaster recovery planning?**

**A:** These days it seems that compliance has a direct impact on nearly everything we do and in a lot of cases with very good reason. Regulatory compliance concerns are, for the most part, designed to protect organizations and individuals from some rather dire consequences, including identity theft and, in the case of the Health Insurance Portability and Accountability Act (HIPAA), health insurance abuse through the unauthorized disclosure of personal information.

#### ***Compliance Impact on Storage***

Regardless of the regulatory compliance concern, it's safe to say that it will in one way or another have an effect on storage, particularly in information management. Information management is the treatment of information acquired by one or many disparate sources in a way that optimizes access by all who can benefit from that information. Compliance may have a broad impact on your organization's information management by predetermining the value of certain types of information. For example, if your organization provides financial services to consumers in the United States, you are subject to the Gramm-Leach-Bliley Act (GLBA), which includes a provision known as the *Safeguards Rule*.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for and plans to continue to protect clients' nonpublic personal information. This plan must include:

- Designation of one or more employees to coordinate its information security program
- Identification and assessment of the risks to customer information in each relevant area of the company's operation, and an evaluation of the effectiveness of the current safeguards for controlling these risks
- Design and implementation of a safeguards program, that includes regular monitoring and testing of the program
- Selection of service providers that can maintain appropriate safeguards, making sure that contracts require them to maintain safeguards and oversee their handling of customer information
- Evaluation and adjustment to the program in light of relevant circumstances, including changes in the firm's business or operations or the results of security testing and monitoring

When you examine the Safeguards Rule in GLBA, several items come to light that may impact the definition of “important” information in information management. For starters, from a storage perspective, you will need to partner closely with the designated employee (or perhaps assign responsible parties from your own area) to coordinate an information security program to protect customer information. Further, you might need to have direct involvement in monitoring and testing of safeguards and assist in the selection of service providers that can maintain appropriate safeguards. It is important to remember that the Safeguards Rule is just one section in a single area of regulatory compliance. Depending upon your organization’s industry, market, and operations areas, many more regulations may apply, each of which bring with them their own unique impacts on the way information (and thus storage) is managed.

### ***Compliance Impact on Business Continuity Planning and Disaster Recovery Planning***

When information is required by business, it is dubbed “mission critical.” When information is required by regulatory compliance, and it is your responsibility to ensure that it’s provided, it goes beyond mission critical to “personal.” Many regulatory compliance concerns can hold internal stakeholders directly accountable for the accuracy and availability of information, and the legal ramifications associated with failing to comply with regulations can be quite significant.

Compliance concerns directly impact business continuity planning during the analysis phase and should be identified as a potential impact during the business impact assessment (BIA) portion of the analysis. The purpose of a BIA is to create a document that can be used to understand what impact a disruptive event might have on the business. Impacts may be financial (quantitative), operational (qualitative), or legal, which is usually a combination of both quantitative and qualitative measures as fines and or disruptions to operations may occur. Compliance concerns present a liability and risk management concern and should be handled as such. In risk management, there are essentially three things that an organization can do with any risk:

- Mitigate—Take actions to eliminate or reduce the risk to an acceptable level
- Offset—Take actions that offset responsibility associated with the risk
- Accept—Accept full responsibility for the risk

During the BIA process, it will be important to correlate the threat of loss with the potential for impact and the perceived outcome that may occur. Once understood, this information can then be used to generate a business case to provide justification to protect against the impact and mitigate the risk. For example, if a regulatory compliance concern has a potential to subject an organization to a civil penalty of \$100,000 USD per loss, disclosure, or misuse of information, and its officers are made personally liable for up to \$10,000 USD (as is the case with GLBA), an additional \$20,000 USD spent per year to protect against this concern may be worth the expense.

The second option is to offset the risk. Depending upon the specific regulatory compliance concern, this may not always be possible; however, it would usually entail making some other party responsible for the portion of the process that presents the risk. For example, if handling medical information in the U.S. is a concern for your organization, you might be able to offset a great deal of risk by partnering with a third-party vendor who could assume the responsibility (risk) of warehousing the information. This may minimize your responsibility to just the information that is accessed by your organization rather than being wholly responsible for all the information.

 In the example given earlier—that the Safeguards Rule makes organizations accountable for “selection of service providers that can maintain appropriate safeguards, making sure that contracts require them to maintain safeguards, and oversee their handling of customer information”—it is important to note that it may not be always possible to offset all the risk. For these and any further questions relating to regulatory compliance responsibilities, it is imperative that your organization contact a skilled attorney, preferably one who specializes in compliance law.

The last option, acceptance, is almost never consciously taken, though many organizations today who claim ignorance of regulatory compliance concerns are doing just that. Risks should only be accepted when their potential to impact the organization can be justifiably offset by the unlikelihood that they might occur or when the cost to deal with the risk is more than the cost of the risk itself. In the case of regulatory compliance, acceptance of risk may, in and of itself, mean violation of the law and should be considered immediate cause for a discussion with an attorney.

## **Q5.2: In an environment of increasingly complicated regulatory and legislative compliance concerns, what steps can be taken to minimize the impact of these concerns on the storage infrastructure?**

**A:** Compliance and litigation introduce some rather complex concerns into the storage environment that will need to be considered as part of an ongoing evaluation of liability and risk management. United States regulatory bodies such as the Securities and Exchange Commission (SEC), Department of Health and Human Services (DHHS), Environmental Protection Agency (EPA), Food and Drug Administration (FDA), and Federal Aviation Administration (FAA) as well international bodies, such as the European Union (EU), have in recent years stepped up monitoring and enforcement of regulations, and the penalties for organization falling out of compliance can be quite severe. In such an environment of increasingly complex compliance concerns, it must be understood that standardization is your friend, variability is your enemy, and complexity should not be feared.

### ***Integrate Compliance Needs into Service and Operating Level Agreements***

Storage architects and administrators depend upon your line of business, data owners, legal, and risk management partners to provide clear information classification. Expectations of data service availability as well as confidentiality and integrity should be given due care during the creation of service level agreements (SLAs) and clearly documented for all parties. Doing so will provide a central point of clarification and clear documentation between line of business partners, records managers, legal counsel, and storage administrators.

### ***Standardizing Product and Service Offerings***

As Q3.2 discussed, standardizing product and service offerings will decrease time to market and provision a more efficient storage infrastructure. Standardization both on external products and services as part of an IT procurement roadmap and internally through standard product and service offerings is key to simplifying the infrastructure—and the more simplified the infrastructure becomes, the more rapidly it can react to changing requirements.

### ***Integrate Compliance in Information Life Cycle Management***

Compliance should play a large role during the information classification phase of information lifecycle management (ILM). Ensure that the appropriate liability and risk management partners are engaged during this process so that information is properly classified.

#### **Q5.3: What major factors influence compliance today and how might they influence storage solutions tomorrow?**

**A:** Regulatory and compliance concerns are generated as an outcome of changes that occur to law or regulations that are enforced through an oversight body, such as the National Association of Securities Dealers (NASD), which is the Self Regulatory Organization (SRO) responsible for the regulation of persons and companies involved in the securities industry in the United States. The underlying question then becomes, “What influences, or drives, the changes in laws and regulations?”

Changes to law and regulations are usually driven by real-world events. The creation of the Sarbanes-Oxley Act (SOX) was driven by a need for reform in business practices in the United States as evidenced by the Enron scandal of 2001. The Health Insurance Portability and Accountability Act (HIPAA) was driven primarily by concerns over patient privacy and the portability of patient information within the health care and health care insurance provider infrastructure. Something usually must happen to trigger a response in the form of a law or regulation to cover a legal contingency. The only exception to this general rule is in the area of merged regulatory discipline. For example, with the formation of the European Union (EU), many different bodies, such as the Financial Services Authority (FSA), Environmental Protection Agency (EPA), and Information Commissioner initially had specific regulatory compliance concerns that in some cases overlap. This makes regulatory compliance in the EU particularly challenging, and future regulatory compliance initiatives may stem from a growing need to consolidate these concerns not only within the EU but also within the international space.

All these factors may drive changes in the underlying laws or regulations, and the storage solutions of tomorrow will need to be prepared. This preparedness will likely manifest itself in a need for greater control, assurance of control, and information security features being demanded within the storage infrastructure.

#### **Q5.4: How do SOX, GLBA, SEC 17A, NASD, HIPAA, and other U.S.-based compliance requirements specifically impact storage and information management?**

**A:** United States-based compliance requirements are going to be of concern not only to U.S.-based companies but also to any international company that wants to do business within the U.S. Each of these major compliance and regulatory concerns will affect organizations differently depending upon the business that is being conducted within the U.S., so let’s examine each of these items as they may impact storage and information management.

### ***The Sarbanes-Oxley Act***

The Sarbanes-Oxley Act of 2002, which is often referred to as SARBOX or simply SOX and is also known as the Public Company Accounting Reform and Investor Protection Act of 2002, is a U.S. federal law that establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. Consisting of 11 titles and including guidance and regulation on corporate board responsibilities, SOX spells out in detail criminal penalties associated with non-compliance. Under SOX, two separate certification sections came into effect—one civil and the other criminal—which are often referred to as sections 302 and 906, respectively.

IT auditors, managers, and storage solutions architects are often most concerned, however, with section 404 of the act, which requires management to produce an “internal control report” as part of each annual Exchange Act report. To provide this report, an audit of the IT infrastructure must take place, and there are two non-exclusive frameworks auditors may use to meet this goal—those produced by the Committee of Sponsoring Organizations (COSO) and Control Objectives for Information and related Technology (COBIT).

### ***The Gramm-Leach-Bliley Act***

The Gramm-Leach-Bliley Act, also known as the Gramm-Leach-Bliley Financial Services Modernization Act or GLBA, is an act of the U.S. Congress that repealed the Glass-Steagall Act and opened up competition among banks, securities companies, and insurance companies. This resulted in a rather broad definition of the term “financial institution,” which now applies to nearly any organization that handles money.

Three provisions within GLBA restrict the collection and use of consumer data and may impact any organization that has a cause to process or store financial data. The Financial Privacy Rule and the Pretexting (also known as Social Engineering) Provisions of GLBA both set forth business practices and apply more to the actual business processes around the handling of consumer financial information than the third provision: The Safeguards Rule requires organizations to implement proactive measures to ensure the security of customer information and most directly impacts storage and information management.

To be in compliance with GLBA, an organization must develop a written information security plan that describes how the company is prepared for and plans to continue to protect clients’ nonpublic personal information. An organization found to be in violation of GLBA may face civil action brought by the U.S. Attorney General the outcome of which can include stiff penalties of as much as \$100,000 USD in fines for each violation. In addition to the organization itself, however, the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than \$10,000 for each such violation. A heavy price to pay when a misconfiguration within a storage or information management setting may lead to hundreds if not thousands or tens of thousands of violations. Like all regulatory and compliance concerns, the key to success is to follow the directions set forth within the act to the letter of the law and implement a sound auditing program to ensure compliance.

## **Securities Exchange Commission Rule 17A**

The Securities Exchange Commission (SEC) Rule 17a-4 requires broker-dealers to create and preserve in an easily accessible manner a detailed record of each securities transaction. These preserved records are used by the SEC to monitor compliance with applicable securities laws, including antifraud provisions and financial responsibility standards.

To ensure compliance with SEC Rule 17a-4, if electronic storage media is used by a member, broker, or dealer, it must comply with the following requirements set forth in sections 2 and 3 of Rule 17a-4:

**Rule 17a-4 Section 2:** If electronic storage media is used by a member, broker, or dealer, it shall comply with the following requirements

i. The member, broker, or dealer must notify its examining authority designated pursuant to section 17(d) of the Act prior to employing electronic storage media. If employing any electronic storage media other than optical disk technology (including CD-ROM), the member, broker, or dealer must notify its designated examining authority at least 90 days prior to employing such storage media. In either case, the member, broker, or dealer must provide its own representation or one from the storage medium vendor or other third party with appropriate expertise that the selected storage media meets the conditions set forth in this paragraph (f)(2).

ii. The electronic storage media must:

A. Preserve the records exclusively in a non-rewriteable, non-erasable format;

B. Verify automatically the quality and accuracy of the storage media recording process;

C. Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and

D. Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.

**Rule 17a-4 Section 3:** If a member, broker, or dealer uses micrographic media or electronic storage media, it shall:

i. At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.

ii. Be ready at all times to provide, and immediately provide, any facsimile enlargement which the Commission or its representatives may request.

- iii. Store separately from the original, a duplicate copy of the record stored on any medium acceptable under Rule 17a-4 for the time required.
- iv. Organize and index accurately all information maintained on both original and any duplicate storage media.
- A. At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.
  - B. Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index.
  - C. Original and duplicate indexes must be preserved for the time required for the indexed records.
- v. The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.
- A. At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.
  - B. The audit results must be preserved for the time required for the audited records.
- vi. The member, broker, or dealer must maintain, keep current, and provide promptly upon request by the staffs of the Commission or the self-regulatory organizations of which the member, broker, or broker-dealer is a member all information necessary to access records and indexes stored on the electronic storage media; or place in escrow and keep current a copy of the physical and logical file format of the electronic storage media, the field format of all different information types written on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.
- vii. For every member, broker, or dealer exclusively using electronic storage media for some or all of its record preservation under this section, at least one third party ("the undersigned"), who has access to and the ability to download information from the member's, broker's, or dealer's electronic storage media to any acceptable medium under this section, shall file with the designated examining authority for the member, broker, or dealer the following undertakings with respect to such records:

## **NASD**

NASD, Inc. whose name was originally the National Association of Securities Dealers but now is referred to simply as NASD, is the primary Self Regulatory Organization (SRO) responsible for the regulation of persons and companies involved in the securities industry in the United States, with delegated authority from the Securities and Exchange Commission (SEC). NASD is not a law but rather a governing body that oversees and regulates trading in equities, corporate bonds, securities futures, and options. Any organization that may trade in these commodities will need to adhere to NASD regulations.

## ***The Health Insurance Portability and Accountability Act***

Unlike SOX and GLBA, which are both primarily concerned with financial information, the Health Insurance Portability and Accountability Act (HIPAA) is focused on medical information and was enacted by the U.S. Congress in 1996. HIPAA is separated into two major sections, referred to within HIPAA as Titles. HIPAA Title I addresses Health Care Access, Portability, and Renewability. HIPAA Title II, however, focuses on preventing health care fraud and abuse, ensuring administrative simplification, and enacting medical liability reform and defines numerous offenses relating to health care and sets civil and criminal penalties for them. Of significant interest to storage and information managers that manage patient information are the Privacy Rule and the Security Rule.

The Privacy Rule establishes regulations for the use and disclosure of protected health information, which is essentially any information related to an individual's health status, provision of health care, or payment for health care. Storage and information architects must be conscious of this concern to ensure that any system designed to operate within a HIPAA environment has the appropriate level of controls in place to meet this requirement.

The HIPAA Security Rule complements the Privacy Rule and lays out three kinds of security safeguards required for compliance. They are:

- Administrative safeguards—Policies and procedures designed to clearly show how the organization will comply with HIPAA:
  - Entities must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
  - Policies and procedures must reference management oversight and organizational buy-in to be compliant with the documented security controls.
  - Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function.
  - Procedures must address access authorization, establishment, modification, and termination.
  - Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to employees performing health plan administrative functions.

- Covered entities that outsource some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements.
- A contingency plan should be in place for responding to emergencies including backup and recovery of data and disaster recovery planning. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- Policies and procedures for internal audit should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.
- Physical safeguards—Controlling physical access to protect against inappropriate access to protected data:
  - Controls must govern the introduction and removal of hardware and software from the network.
  - Access to equipment containing health information should be carefully controlled and monitored.
  - Access to hardware and software must be limited to properly authorized individuals.
  - Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
  - Policies are required to address proper workstation use. Workstations should be removed from high-traffic areas and monitor screens should not be in direct view of the public.
  - If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.
- Technical safeguards—Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:
  - Information systems housing PHI must be protected from intrusion. Encryption is required when communicating beyond the local network.
  - Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
  - Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
  - Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be.
  - Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.

- In addition to policies and procedures and access records, IT documentation should include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
- Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act.

### Q5.5: What steps can I take to ensure compliance in my environment?

**A:** The first step to ensuring compliance is to accurately understand each compliance concern your organization may be faced with and implement the appropriate response. Question 5.4 covered many United States-based compliance concerns, and Question 5.6 addresses several international concerns, but neither list is all inclusive. There may still be further compliance concerns faced at the international, national, or regional level, so the first step in ensuring compliance in your environment is to understand the outside factors that may impact your organization and take steps to comply with all applicable laws. Once your organization takes action to comply, the only way to ensure compliance is to be audited by the same standards upon which your organization will face by an external auditor. Two of the most common methods used by auditors are Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Control Objectives for Information and related Technology (COBIT).

#### COSO

COSO is a U.S. private-sector initiative formed in 1985 to identify the factors that cause fraudulent financial reporting and make recommendations to reduce its incidence, which directly compliments the Sarbanes-Oxley Act (SOX) legislation. COSO has released IT auditing guidelines that are commonly referred to as simply “COSO” and focus on five key areas:

- Control environment—Control environment factors include the integrity, ethical values, management operating style, delegation of authority systems, and the processes for managing and developing people in the organization.
- Control activities—Control activities are the policies and procedures that help ensure management directives are carried out. They include a range of activities including approvals, authorizations, verifications, reconciliations, and reviews of operating performance, security of assets, and segregation of duties.
- Information and communication—Information systems and communications are central to the reporting process for operational, financial, and compliance-related information. The flow of information via communication with external parties, such as customers, suppliers, regulators, and shareholders must be maintained to ensure compliance.
- Monitoring—Internal control systems need to be monitored—a process that assesses the quality of the system’s performance over time. This is accomplished through ongoing monitoring activities or separate evaluations.
- Risk assessment—Risk assessments are a prerequisite for determining how the risks should be managed.

## COBIT

COBIT is a framework of best practices for IT management created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992.

Currently in version 4, the COBIT Framework is generally accepted as being one of the most comprehensive works for IT governance, organization, and process and risk management.

COBIT provides effective practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of enterprise management by bridging the gaps between business risks, technical issues, control needs, and performance measurement requirements.

COBIT defines IT activities in a generic process model within four domains:

- **Plan and Organize (PO)**—This domain covers strategy and tactics and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated, and managed for different perspectives. Finally, a proper organization as well as technological infrastructure should be put in place.

This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organization understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?
- **Acquire and Implement (AI)**—To realize the IT strategy, IT solutions need to be identified, developed or acquired, and implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives.

This domain typically addresses the following management questions:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?
- **Deliver and Support (DS)**—This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities.

It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimized?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity, and availability in place?

- **Monitor and Evaluate (ME)**—All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance, and providing governance.

It typically addresses the following management questions:

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are risk, control, compliance, and performance measured and reported?

Auditing your environment with either one of these standards as a framework will help to ensure that your organization remains compliant. Depending upon the size and footprint of your company, you might want to hire and maintain an internal staff of auditors to accomplish this task, but routine external auditing should still take place on a regular basis to ensure nothing is overlooked.

## **Q5.6: How do international standards, such as the United States DoD 5015.2, ISO 15489, and MoREQ, effect storage and information management requirements and implementations?**

**A:** International standards such as DoD 5015.2, ISO 15489, and MoREQ all have the potential to impact storage or information management systems in the global space: DoD 5015.2 for any application that may need to interface or interact with a United States Department of Defense (DoD) system, ISO 15489 as a generally accepted standard for records management, and Model Requirements for the Management of Electronic Records (MoREQ) as a European standard for electronic records management systems. Let's examine each of these standards and how they may impact storage and information management requirements for your organization should it have a need to operate in this space.

### **DoD 5015.2**

DoD 5015.2 is a records management certification managed by the Joint Interoperability Test Command of the U.S. DoD. Under this article, there are actually two separate and distinct certifications: Chapter 2 and Chapter 4. Certification under Chapter 2 entails certification of mandatory criteria that is required by all records management applications used by U.S. government agencies, and Chapter 4 is specific to applications that process classified records.

Both certifications can be quite arduous and if your organization has no need to interact directly with the U.S. DoD in a records management capacity, you may not be inclined to attempt to ensure this level of records management certification. DoD 5015.2, however, does provide very specific requirements that will benefit any organization that has a desire to formalize and manage its records management program. Although the full detail of DoD 5015.2 is quite lengthy, the general requirements for a records management application (RMA) are provided here to illustrate some of the effects this standard may have on information management.

### 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)).

### ISO 15489

ISO 15489 was the first international standard to address records management and provides a comprehensive basis for auditing full and partial records management programs. ISO 15489 provides a framework for planning and implementing a records management program and includes provisions for:

- Setting policies and standards
- Assigning responsibilities and authorities
- Establishing and promulgating procedures and guidelines
- Providing a range of services relating to the management and use of records
- Designing, implementing, and administering specialized systems for managing records
- Integrating records management into business systems and processes

## MoREQ

MoREQ an international specification that focuses mainly on the functional requirements for the management of electronic records. Throughout the various sections of MoREQ, several areas of interest to storage and information management emerge, including access control, email security, encryption, performance and scalability, and metadata specifications—all of which may have a significant impact on storage and information management. Key areas of focus within the MoREQ specification include:

- **Classification Scheme**—The Classification scheme defines the way in which the electronic records will be organized into electronic files and the relationships between the files.
- **Controls and Security**—Specifies controls and security as it relates to access, audit trails, backup and recovery, tracking record movements, authenticity, and security.
- **Retention and Disposal**—Includes specific guidance on the retention schedule, review, transfer, export, and destruction of data.
- **Capturing Records**—Covers the capture, bulk importing of files (data), the types of documents to capture, and email management.
- **Referencing**—Provides guidance on references within the electronic records management system, such as classes, files, volumes, and records—all of which need identifiers in order to be referenced appropriately.
- **Searching, Retrieval, and Rendering**—Provides the defined specifications on record search, retrieval, and rendering, including displaying records, printing records, and any other form of possible render (identified as ‘other’ within the specification).
- **Administrative Functions**—Covers general administration and reporting and the changing, deleting, and redacting of records.
- **Other Functionality**—Provides specifications related to topics not covered within previous sections of the specification, including management of non-electronic records, hybrid file retention and disposal, document management, workflow, electronic signatures, encryption, electronic watermarks, interoperability, and openness.
- **Non-Functional Requirements**—The MoREQ specification acknowledges that not all attributes of a successful system can be defined in terms of functionality. These requirements fall into the non-functional portion of the specification and include ease of use, performance and scalability, system availability, technical standards, legislative and regulatory requirements, outsourcing and third-party management of data, long-term preservation, and technology obsolescence.
- **Metadata Requirements**—The metadata requirements provide specific guidance on indexing information and other data such as access restriction information. This includes principles, classification scheme metadata elements, class and file metadata elements, metadata elements for file or file volume, volume metadata elements, record metadata elements, record extract metadata elements, user metadata elements, and role metadata elements.

## **Q5.7: What best practices or guidelines exist that can help ensure corporate governance?**

**A:** Ensuring corporate governance, or more specifically corporate IT governance, is a central theme throughout many regulatory and compliance concerns. Someone, some office, or some small group must be held accountable for the actions of the organization. The concept is not unique, however, to compliance. Good management practices dictate the same logic. Roles and responsibilities must be clearly defined and people need to be responsible and accountable for their actions. So how can you help ensure corporate governance?

### ***Build a Culture of Accountability***

Regulatory compliance often thrusts financial accountability on to the organization or in the case of the Gramm-Leach-Bliley Act (GLBA), onto individuals within an organization. Although extremely motivating, financial accountability cannot be enforced throughout most organizations; after all, an organization would have a hard time maintaining employee morale with a “you break it, you bought it” mentality on compliance. It is possible, however, to encourage associates to be emotionally accountable. Being accountable in its most basic definition means not only to be responsible for something but to answer to its shortcomings. The parent of a child who gets in trouble is more than just responsible for the child, they often become accountable for the incident and are motivated to be accountable not out of any financial driver but out of their love for the child. This level of emotional accountability can be built within a corporate culture by developing leaders that are willing to be part of an accountable process. Unlike responsibility, you can’t force someone to be accountable. It is more of a proactive state of responsibility. You can, however, grow and incent leaders that take accountable action.

### ***Emphasis Process over People***

Emphasizing process over people is often misunderstood as being anti-people. On the contrary, by empowering process over people, an organization removes many barriers, or roadblocks, to individual success by limiting an individual’s responsibility and accountability to their level of control over a process—which is both freeing to the individual and conducive to teamwork and process-centric business practices. Not many people, for example, would be comfortable identifying, defining, measuring, analyzing, implementing, and then performing post-implementation control over a \$100 Million USD application system. It would be quite literally an onslaught of responsibility and the work effort alone would require so many differentiated roles that no one person could effectively run the entire operation as efficiently or effectively as a team of engineers, project managers, service delivery managers, and business support. By emphasizing process over people leadership, responsibility and accountability can be portioned out in a manner that ensures positive control over IT while ensuring the best people are in place within the process and don’t become overwhelmed.

---

### **Identify Strategic Value**

Determining “strategic value” is likely to be one of the most difficult jobs within any organization. After all, it is quite rare that a project jumps off the page at the decision maker’s desk and clearly make its case for why it’s important to the enterprise. Identifying strategic value, however, is key to ensuring corporate IT governance. Without this understanding, decisions often appear as if they’re made within a vacuum with little or no consensus among stakeholders.

So how can your organization fight to identify strategic value? First, make sure all the key stakeholders are at the table. Understanding strategic value is going to require a clear understanding of what is strategically important to all line of business areas. A design and engineering team’s best idea, for example, is completely useless unless the shipping department can box it up and send it out the door. Drive for a holistic view that weighs the needs of all the stakeholders and then determine which projects are implemented based upon that understanding.

### **Set Clear Priorities**

It seems that most organizations these days are in a constant state of change. Although change in and of itself is often good, it can be over done and too much change can cause associates to lose track of priorities in the process. No one could conceive a medical doctor accepting a new teaching position and his first action once he hears about it is to walk out of the operating room in the middle of a surgery to study; yet in many organizations, IT managers do exactly that. The reason why is a clear lack of priorities. Determine what is a priority for your organization, or even for your department or yourself, and set clear guidance on how to maintain those priorities. A financial institution, for example, may have concerns around regulatory compliance, customer feedback, and privacy, but all these are just secondary to the clear priority of “ensuring the customer trusts us.” If a bank, for example, lost the trust of the public, everything else would be in ruin. Set and maintain clear priorities.

### **Audit Often**

Many organizations have a very positive perception of themselves. No one likes to think that they work for a sloppy organization, so oftentimes, whether it be under the guise of morale or team spirit, we allow our organizational ego to get inflated. Although it may feel good, it is often vanity. Auditing of the infrastructure for compliance with applicable regulations is necessary to keep that vanity in check.

## **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>.