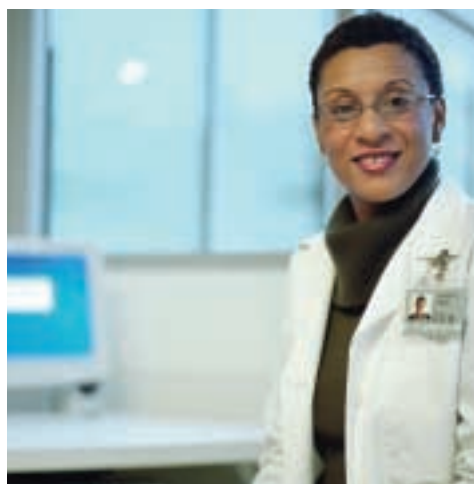


ENTERPRISE STORAGE SOLUTIONS

# NETAPP REGULATORY COMPLIANCE SOLUTIONS



## REGULATORY COMPLIANCE SOLUTION

Network Appliance delivers comprehensive compliance solutions to address your business needs. Through a combination of products, services, and partnerships, NetApp compliance solutions help mitigate risk, simplify data management, and deliver investment protection.

An ever-increasing number of digital assets that your organization retains for active reference are subject to regulatory compliance. NetApp provides your organization with regulatory compliance solutions that can mitigate risk, simplify data management, and benefit your bottom line.

## Market Overview



The impact of regulatory compliance on the global IT community is enormous. It may pose the biggest challenge ever faced by your IT organization.

Regulatory scrutiny has become increasingly aggressive. It is estimated that more than 10,000 compliance regulations exist globally. These regulations describe the process by which records must be created, stored, accessed, retained, and destroyed over increasingly long periods of time—in some cases longer than a human lifespan. Enforcement of these regulations has become a well-funded high-priority item in the wake of recent events surrounding corporate scandals and high-profile privacy and security breaches. Implementing a solution to address the regulatory compliance challenge is not optional, as failure to do so can put your company out of business. Fines totaling billions of dollars have been handed out in recent years. Although the data subject to regulatory compliance regulations varies by industry, one can generalize that many records pertaining to your daily business, such as activities and correspondence between organizations, employees, and individuals, are subject to compliance regulations. These records might include financial and other digital records, medical images and data related to personal patient

health information, digital audio and video files, and e-mail messages and archives.

Corporate executives and IT managers face a dilemma: divert scarce resources to cover increased management and storage costs or accept the risk of regulatory enforcement actions and penalties. As IT professionals, the goal of your regulatory compliance strategy must be to minimize your company's exposure to litigation, fines, and reputation damage—all while minimizing costs.

Data storage is a major component of any regulatory compliance process. The new regulations mandate that you retain your data for significantly longer periods of time. The spiraling expansion of this compliance data will change your business's fundamental IT infrastructure. Your business has to manage several concurrent requirements, which often seem at odds with one another:

- You need to provide information to authorized users anywhere, anytime
- You need to reduce the potentially catastrophic risk of noncompliance by strictly complying with regulations
- You need to keep your costs down
- You need to create ways to leverage the new data to benefit other areas of the business

# Impact of Regulations on Storage



Although each of the thousands of regulations is unique, there are three recurring themes that have a direct effect on a company's storage strategy.

The first of these is data permanence. This is the concept that data must be saved to media that cannot be altered or erased until a specified expiration date. The data permanence requirement is particularly important in the financial services industry as a result of heightened scrutiny by the SEC and other law enforcement authorities. SEC Rule 17a-4 mandates data permanence for "all communication (internal or external) related to the business as such." Although the financial industry has perhaps the most explicit mandate for data permanence, it is by no means the only industry finding data permanence to be a necessary component of a regulatory compliance solution.

The second is data security. Security requirements vary widely, but almost every entity is subject to some type of security regulation. For example, the healthcare industry is subject to the HIPAA security regulations. They are intended to protect patient privacy. Because of this, data security measures

such as access controls and encryption are strongly encouraged as approaches to complying with the regulation. In fact, privacy tends to be a large area of regulatory focus. These regulations range from the EU Data Protection Act (affecting all European businesses), which is focused on employee privacy, to the Gramm-Leach-Bliley Act (affecting the U.S. financial industry), which protects the privacy of U.S. consumers. A successful regulatory compliance solution will be able to support privacy requirements such as authentication and access control.

The third is auditability. The life sciences industry illustrates this requirement. 21 CFR Part 11 is an FDA (Food and Drug Administration) regulation that outlines the requirements for dealing with electronic records and signatures. Having a secure audit trail is at the heart of this requirement. Every access and modification to an electronic record has to be maintained. The auditability requirement is common in compliance regulations across industries.

## Considerations for Selecting a Storage Solution

Obviously, any regulatory compliance storage solution must address the data permanence, security/privacy, and auditability requirements of your business. However, there are additional criteria to consider. Choosing a regulatory compliance storage platform is a very strategic decision. Your regulatory compliance data will have to be maintained for years to come, and the underlying storage needs will have to fit into your storage management strategy. Some areas to consider:

**Reliability.** Losing the data could jeopardize your company.

**Performance.** While the storage does not need to be as high performing as primary storage, the inability to recover data in a timely fashion is likely to result in significant financial penalties.

**Open standards.** If the storage does not operate on a well-known standard such as NFS or CIFS, applications will have to be specifically tailored to work via a proprietary API. This will limit your options now and in the future.

**Investment protection.** Do you have to purchase dedicated hardware for regulatory compliance, or can you leverage storage devices that are also used for other applications such as backup and primary storage? This is particularly important when considering smaller offices.

**Security.** Obscurity is not security. Is the storage solution secured by well-known hardened protocols such as Kerberos and IPSec?

**Scalability.** Can you start small and grow the same solution with increasing business demands?

**Migration.** Can data easily be migrated on or off the device? If not, you are likely to have a vendor lock-in issue in the future. Regulatory compliance data will likely outlive the storage device due to long retention requirements.

## The NetApp Solution

At Network Appliance we have been working with our customers, partners, and third parties to develop, assess, and validate regulatory compliance solutions that not only satisfy existing regulations, but also provide flexibility and attractive total cost of ownership. Working closely with our customers, we developed solutions that minimize risk while maximizing your total investment. All of our regulatory compliance solutions are available across the complete family of NetApp systems. This allows for a large data center to leverage a NetApp NearStore® system for compliance, replication, and backup, while a smaller office can utilize its existing FAS server (e.g., the FAS250) to meet its compliance needs. The entire solution interoperates (e.g., for replication and management) seamlessly.

### DATA PERMANENCE

NetApp SnapLock™ provides the most flexible data permanence solution currently available. Using standard NFS and CIFS network access protocols, SnapLock gives your company a way to utilize any NetApp system to meet the data permanence requirements. Widely deployed for the most stringent regulatory requirements such as SEC Rule 17a-4, SnapLock provides a way to guarantee data permanence at a file level. Interoperability with your applications (third-party or in-house) is simple, and all standard features of a NetApp system (such as SnapMirror® for off-site replication) are preserved.

### DATA SECURITY

NetApp compliance solutions offer a holistic approach that effectively addresses security and privacy concerns specific to data storage. Significantly, the Network Appliance™ Data ONTAP™ operating system features strong native security features to ensure that data is accessed only in the ways that were intended. Our security is based on industry standards such as LDAP, Kerberos, SecureAdmin™, and IPSec. Recognizing that some industries (e.g., the defense industry) mandate even stronger protection, NetApp has

partnered with Decru to optionally offer military-grade encryption. This approach highlights the NetApp philosophy of partnering to offer best-of-breed solutions.

### AUDITABILITY

Auditability is best achieved via a combination of hardware and software. The NetApp Data ONTAP operating system natively supports all industry-standard auditing features. NetApp has partnerships with industry-leading solution providers such as Princeton Softech for structured data (e.g., databases); KVS, IXOS, and FileNet for semistructured data (e.g., e-mail); and VERITAS for unstructured data (e.g., home directories). Together with our partners, NetApp offers your company solutions that are truly best of breed.

## The NetApp Advantage

There is no single product from any vendor that will address all your compliance needs. However, NetApp offers comprehensive regulatory compliance storage solutions that will help you comply and better compete in the ever-competitive global marketplace while establishing data management procedures that are best in class. In addition, NetApp provides other benefits such as storage consolidation; better data sharing; lower total cost of ownership; and more efficient use of disk, tape, and optical storage. Our differentiating features include:

### FLEXIBILITY

From the primary data center to a branch office, NetApp compliance solutions have the flexibility to meet your needs. Regardless of the specific regulatory requirements of your industry, your current business model, your current storage solution, and the amount of data you are storing, NetApp offers a solution. NetApp solutions allow you to store regulatory compliance data and other types of data on the same system. This flexibility provides investment protection and ensures that your regulatory compliance solution fits into your existing storage strategy regardless of location or size.

#### **OPEN STANDARDS**

NetApp uses open standards such as NFS and CIFS. This helps guarantee interoperability with existing and future applications while ensuring that data migration, management, and backup will be nonissues.

#### **APPLICATION INTEGRATION**

Because NetApp uses open standards such as NFS and CIFS, you can be sure that applications will integrate easily. This is an important consideration not only for commercial applications that your company currently uses, but also for “homegrown” and future applications.

#### **PERFORMANCE**

Many times performance is an afterthought when evaluating regulatory compliance solutions. This can be a critical mistake. While it is true that regulatory compliance solutions rarely demand the high performance of a production database, it is very critical that whatever solution you choose can recover records quickly enough to satisfy demands from the regulatory authorities. NetApp solutions excel not only in raw throughput, but also in the ability to service many simultaneous, random recovery requests.

#### **CREDIBILITY**

NetApp is a market leader in providing storage solutions to help companies satisfy regulatory compliance requirements. NetApp solutions have successfully endured rigorous scrutiny, including DoD 5015.2 and the SEC Rule 17a-4.

#### **TOTAL COST OF OWNERSHIP**

NetApp can scale up or down with compliance solutions that leverage your existing investment. Our solutions

integrate with small installations and existing NetApp FAS servers or with large, new installations using NetApp NearStore systems. You can use a single FAS server or NearStore system for both regulatory compliance and your everyday storage requirements.

#### **MANAGEABILITY**

NetApp solutions can be managed using the existing data storage management approaches. This includes using existing backup, replication, and monitoring paradigms. This translates into less risk and lower TCO. NetApp can provide one compliance solution across the entire enterprise.

#### **RELIABILITY AND SCALABILITY**

NetApp regulatory compliance solutions offer the reliability NetApp is known for. The field-measured average availability of all NetApp nonclustered systems is 99.995%. Clustered systems provide even higher availability. With NetApp, you can start at as small as .5TB and grow on a single system to 96TB.

#### **UNIFORMITY IN ARCHITECTURE**

All NetApp systems, primary or nearline, small or big, have the same operating system and architecture. This uniformity in architecture simplifies data management tasks in data centers and remote offices. For example, small FAS systems in multiple branch offices can all mirror to a single large NearStore system in the data center, without any manual intervention. Furthermore, the same FAS systems with compliance storage in remote offices can also serve e-mail using a block protocol and serve file via a file protocol such as CIFS.

#### **SECURITY**

NetApp storage systems provide native enterprise directory support for consistent authentication, IPsec, strong (military-grade) encryption support, granular (record-level) access controls and restrictions, specific network and port restrictions, and storage-centric audit-logging capability. The NetApp Operating System (Data ONTAP) has been field-proven for over 12 years for effective security.

#### **INVESTMENT PROTECTION**

NetApp solutions protect your investments by nondisruptively fitting into your existing backup and archival infrastructure in tape or optical jukeboxes. A NetApp solution that is purchased for compliance can also be leveraged as part of a backup or disaster recovery solution. Further, moving from an older NetApp platform to a newer NetApp platform is easy, thanks to our open standards and technology such as SnapMirror. A NetApp solution prevents vendor lock-in while ensuring that your investment is fully leveraged, now and in the future.

NetApp works actively in the compliance community and meets often with regulatory agencies to ensure that our solutions are able to help organizations meet regulatory requirements should regulations change in the future.

## NetApp Compliance Solutions Matrix

Following is a matrix listing industries impacted by compliance regulations, followed by applicable regulations for each and the relevant NetApp solution:

REGULATION	REGULATORY AGENCY	ORGANIZATIONS IMPACTED	REQUIREMENTS	NETAPP SOLUTION
17CFR (Code of Federal Regulations) 240.17a-4 (or 17a.4)	Securities and Exchange Commission (SEC)	Financial services	Type and length of data retention, storage media requirements	SnapLock (for data permanence) combined with a NetApp system such as NearStore or FAS. Typically back-ends e-mail archival or document archival applications.
21CFR (Code of Federal Regulations) Part 11	Food and Drug Administration	Pharmaceuticals, medical device manufacturers	Security, integrity, auditability	A NetApp system featuring Data ONTAP native security optionally combined with SnapLock for data permanence. Typically works in conjunction with records management software from a partner.
Basel Capital Accord (or Basel II)	G-10 nations	Financial services	Reduce operational risk	Built-in resiliency and self-healing features of NetApp systems combined with SnapMirror for off-site data protection and reduced operational risk.
California Senate Bill 1386 (or SB 1386)	State of California	Financial services that do business in the state of California	Protect consumer privacy	A NetApp system featuring Data ONTAP native security. Optionally add Decru DataFort for strong encryption.
Data Protection Act(s)	European Union, UK Data Commissioner	European operations, global firms	Protect privacy (particularly employees)	A NetApp system featuring Data ONTAP native security. Optionally add Decru DataFort for strong encryption.
DoD 5015.2-STD	Department of Defense	U.S. military branches	Strong authentication, auditability, and encryption	NetApp systems for primary and backup storage with SnapMirror (for off-site backup), and Decru DataFort for encryption and crypto-shredding. Optionally add SnapLock for data permanence.
Gramm-Leach-Bliley Act (or GLBA)	Federal Trade Commission (FTC)	Financial services	Encryption, secure backup, data destruction	A NetApp system featuring Data ONTAP native security. Optionally add Decru DataFort for strong encryption and crypto-shredding.
HIPAA (Health Insurance Portability and Accountability Act)	U.S. Health and Human Services	Health insurance, healthcare providers	Privacy, security, very long retention periods	NetApp storage systems combined with SnapMirror for data protection. Optionally add SnapLock for data permanence.
Sarbanes-Oxley (or SOX)	Securities Exchange Commission	Public companies, accounting firms	Reliability, data protection, data permanence to protect against alteration or destruction of data	NearStore or FAS systems combined with SnapLock for data permanence.



**Network Appliance, Inc.**  
495 East Java Drive  
Sunnyvale, CA 94089  
www.netapp.com

© 2004 Network Appliance, Inc. All rights reserved. Specifications subject to change without notice. NetApp, the Network Appliance logo, NearStore, and SnapMirror are registered trademarks and Network Appliance, Data ONTAP, SecureAdmin, SnapLock, and The evolution of storage are trademarks of Network Appliance, Inc. in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. **RC-001-0304**