



*Building Best Practices  
in Records Management  
Compliance:*

*ILM strategies for security, protection,  
recovery and availability*

## Overview

There has been greater awareness within recent years regarding record retention and management guidelines in the financial sector. While certainly deserving of consideration, this increase doesn't signify an emerging school of thought or entirely new chapter in industry regulatory scrutiny. In fact, neither the concept nor the specific concern is at all novel. However, the transition from legacy, manual and paper-based processes to digital and electronic systems is relatively recent—and it has affected application and interpretation of existing guidelines and best practices focused on this area. In other words, the attention currently being paid to information management policy and execution by the financial industry is recognition that it needs to address issues associated with a predominance of electronic records and its reliance on technology to maintain and archive data.

It's a classic chicken and egg. IT is the enabler and primary vehicle for the creation and storage of modern records. But it also simultaneously represents the biggest obstacle to and the best method for ensuring the privacy, validity and integrity of corporate information throughout its lifecycle—from creation through active use and then into a period of long-term retention.

Take the Securities and Exchange Commission (SEC) Rule 17a-4 as an example. Part of the Securities Exchange Act of 1934 (“The 1934 Act”)—which extended federal regulation of securities trading past the limited scope of the Securities Act of 1933 (“The 1933 Act”)—the rule is 70 years old. And, Rule 17a-4 is merely an original section within that legislation that requires every national securities exchange member, broker and dealer to keep accessible records made between certain parties for specified periods of time. The spirit and intent of this section may not have not changed much or at all since 1934, but interpretation and relevance have certainly evolved along with financial industry automation—making compliance today more of a challenge.

*“In response to cited email archiving violations of SEC 17a-4, five of the largest investment banks in the world (Goldman, Sachs & Co., Citigroup Inc.’s Salomon Smith Barney, Morgan Stanley & Co., Deutsche Bank Securities Inc., and U.S. Bancorp Piper Jaffray Inc.) have agreed to pay a fine of more than \$8 million.”*

*Source: Wall Street Journal, August 2, 2002*

## Challenges for Information Technology and Availability

For many financial institutions, this challenge is compounded by growing regulatory scrutiny of the information management function, which in turn, is the result of rising industry concern. From “backdating” sales of more than \$1 billion to improve a major software company’s financial statements to a censure and fine of \$10 million for an international securities firm’s failure to furnish certain requested records, there is significant cause for alarm. And, financial sector regulatory agencies are taking notice—enacting guidelines impacting record management, including:

- Section 103 of the Sarbanes-Oxley Act (SOA) of 2002, which mandates that accounting firms retain for seven years records relevant to the audit and financial statement review functions.
- National Association of Securities Dealers (NASD) Conduct Rule 3010(d)(3) and Conduct Rule 3110(a) of 2002, which dictate that members retain correspondence of registered representatives relating to investment banking or securities and make and preserve books, accounts, records, memoranda and correspondence in conformity with all applicable laws, rules, regulations and statements as prescribed by SEC Rule 17a-3 and in a format, medium and retention period that complies with SEC Rule 17a-4.

Because of the potential for huge fines—not to mention market brand perception and erosion of shareholder value that come from negative publicity—financial institutions need to take compliance and audit of applicable information management rules very seriously. Experts have estimated cumulative organizational penalties to grow to \$500 million to \$1 billion for SEC 17a-4 infractions. In response to cited email archiving violations of that rule, for instance, five of the largest investment banks in the world (Goldman, Sachs & Co., Citigroup Inc.’s Salomon Smith Barney, Morgan Stanley & Co., Deutsche Bank Securities Inc., and U.S. Bancorp Piper Jaffray Inc.) agreed to pay a fine of more than \$8 million, in addition to reviewing and reporting on their procedures for email retention.

When it comes to records management and retention, governing bodies and auditors are looking for accuracy and integrity as demonstrated by chains of custody, the ability to preserve that chain for evidence purposes, instituted controls for retention for specific periods of time and reasonably fast and easy retrieval. SEC Rule 17a-4 specifically requires:

- Written and enforceable retention policies
- Storage of data on indelible, non-rewriteable media
- Searchable index of all stored data
- Readily retrievable and viewable data
- Storage of data offsite

That’s a fairly tall order for IT and an enormous burden on an information availability plan. But boiled down to its essence, this regulation requires a comprehensive program that addresses information security, protection, monitoring, maintenance and exchange.

### *What this Means to You*

To that aim, you need to review your information availability plan to ensure support of effective and efficient information management throughout its lifecycle. Beyond the more obvious areas of data continuity and recovery, you should examine the larger suite of covered electronic records, including emails and instant messages (IMs). Finally, you must articulate and define rules, strategies and evaluations for record retention of both structured and unstructured data, and ensure your underlying infrastructure is capable of supporting them. At a minimum, you need to:

- Guarantee that your strategy includes policies, procedures and supervision for appropriate record security, replication, protection, recovery and availability
- Establish a framework for management and monitoring of your solution hardware, network, security, and storage that supports that strategy

## Supporting Compliance with Information Availability Planning

Records management compliance programs are incomplete if they do not adequately address information availability within the larger information lifecycle management plan. The emphasis of the rules on prolonged retention and easy accessibility mean business continuity (BC), disaster recovery (DR) and IT infrastructure are very real areas of concern. More to the point, existing information availability plans must be reviewed and modified to ensure and support the required level of records security, protection, monitoring, maintenance and exchange.

Without the appropriate accommodation in those areas, a records management program is neither complete nor truly lifecycle based. To be both, the program must support record creation, active use and long-term retention—and information availability as it relates to those areas. That means you need to consider the following six areas in your comprehensive information lifecycle management program:

1. Secure, trustworthy around-the-clock server and application management
2. Comprehensive protection and risk mitigation
3. Comprehensive scalable storage for such diverse records containing conclusions, opinions, analyses and financial data as work papers and emails, computation notes and instant message communications
4. 24/7 performance and availability monitoring
5. Fast, reliable, on-demand access to a protocol-independent network
6. Comprehensive record continuity and recovery planning

### *Deriving best practices from information management rules*

In addition to helping identify the means to comply with multiple regulations, an in-depth review of the significant information management rules reveals some of most progressive theories regarding record security, replication, protection, recovery and availability. And, these prevailing schools of thought can serve as your benchmark and guide to improving your overall program. By embracing the sum total of guidelines affecting the function, you can harness the inherent benefits of common goals and an active marketplace of ideas.

Building an information management program that reflects the best of multiple standards all but guarantees that it will include progressive thought regarding record security, replication, protection, recovery and availability. Moreover, instituting a solution that strives to comply with one or more industry regulations is an easy and inexpensive way to achieve cross-the-board compliance.

Following is a brief list of reference rules for information lifecycle management:

- SEC Rule 17a-4, 1934—States that every national securities exchange member, broker and dealer is required to keep accessible records made between certain parties for specified periods of time.
- Foreign Corrupt Practices Act (FCPA), 1977, 1988—In order to eliminate bribery and make illegal the destruction of corporate documents to conceal a crime, requires corporations to “... make and keep books, records and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets...”
- Food and Drug Administration (FDA) Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application, 1997—Provides guidance “to persons who, in fulfillment of a requirement in a statute or another part of FDA’s regulations to maintain records or submit information to the FDA” on protection requirements to enable accurate and ready retrieval throughout a mandatory retention period.

## Conclusion

Now is a perfect time to examine and improve your information management program in order to ensure you've addressed the pertinent lifecycle issues. Success depends upon the ability to initiate and maintain a disciplined methodology that reflects your institution's needs for compliant record security, replication, protection, recovery and availability, which amounts to a significant review of your information availability program.

You should begin the process with a thorough evaluation of your current program through a risk assessment and technology profile. With those insights, you can effectively evaluate, develop and execute your plans for compliance and help ensure that you can support it with BC, DR and robust infrastructure.

SunGard experts can assist you at every step of the way—from assessing your existing data integrity and availability to creating and implementing a plan for hardware, network, security and storage improvement. To get started today on your path to a comprehensive information management program, call our information availability experts at 1-800-434-0002 or visit our website at [www.availability.sungard.com](http://www.availability.sungard.com).

- Section 103 of the Sarbanes-Oxley Act (SOA) of 2002— Requires accounting firms to retain records relevant to the audit and financial statement review functions for seven years.
- NASD 3010(d)(1), 2002—States that a firm must establish procedures in writing for how electronic correspondence between their registered representatives and the public are recorded. A key part of these policies specify supervisory roles and require that a registered principal review incoming and outgoing email.
- DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications, 2002—Sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by Department of Defense (DoD) Components in the implementation of their records management programs, defines required system interfaces and search criteria to be supported by the RMAs and describes the minimum records management requirements that must be met, based on current National Archives and Records Administration (NARA) regulations.
- USA Patriot Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, 2001 (Sec. 1016) — Critical Infrastructures Protection Act of 2001 — Declares it is U.S. policy: that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and U.S. national security; that actions necessary to achieve this policy be carried out in a public-private partnership involving corporate and non-governmental organizations; and to have in place a comprehensive and effective program to ensure the continuity of essential Federal Government functions under all circumstances.

Specific SunGard services, which are itemized below can help you comply with the various information management regulations affecting the financial industry. These services expand on the consideration areas presented previously.

## SunGard Services

### *Availability Architecture Services—Objective advice on information availability issues*

**IA Options Analysis**—Outlines and examines the full spectrum of available options for disaster recovery

**Recovery Strategy Design and Implementation**—Provides an in-depth, drill-down plan for implementing a first choice for a recovery solution

**High Availability Solutions**—Options analysis, strategy, design and implementation services of available choices

**Storage Architecture Solutions**—Design and implementation of a technology architecture that helps ensure back up of large amounts of data more quickly and effectively

**Network Availability Solutions**—Analysis of the current network environment, implementation and testing of a recovery network configuration and design of the high availability network component

### *Information Security Services—Objective advice on data protection and risk mitigation*

**Program Review**—Review of an existing security program

**Program Assessment**—Review of an existing security program, including comparisons and recommendations

**Policy and Procedure Design**—Development of tailored Information Assurance policies, standards and procedures

**Penetration Assessment**—A comprehensive approach that covers external, internal, and wireless testing

**Vulnerability Assessment**—Technical assessment of an entire infrastructure

**Network Architecture Review**—A thorough review of the security of network topology, firewall and router rule sets, as well as remote-access solutions

**Alternate Site Vulnerability**—A security test focused on the organization's alternate recovery environment

### *Validation and Testing Services— Objective advice on a wide-range of technology issues*

**Tape Review and Audit**—Help in prioritizing and creating a formal escalation process, in addition to a backup and review session before a test

**Procedure Development**—Interviews of personnel to build detailed recovery procedures for systems and data

**Backup Strategy Analysis**—Analysis of an existing backup infrastructure

### *System Management Services—Around-the-clock server and application management*

**Secure Server—Operating System Support**—Designed to support the integrity of the operating system to help ensure maximum uptime and availability

**Secure Server—Database Support**—Developed to help support customers' database servers and to help the capital investment required to build the state-of-the-art management fabric required to properly monitor an infrastructure

### *Managed Security Services—Outsourced ownership of protection and risk mitigation*

**Managed Firewall**—Installation, configuration and management of firewall hardware and operating system software

**Managed IDS**—Installation, configuration and management of hardware and software to monitor, detect and respond to system intrusions around the clock.

**Managed Vulnerability Protection**—Periodic assessments that search for vulnerabilities and seek out security holes

### *Managed Storage Services—Outsourced ownership of the data storage function*

**Managed Tape Backup**—A complete solution that includes software, media and off-site protection

**Managed SAN Services**—A shared storage platform for an "always-on" Managed Storage Utility

**Replication Services**—Real-time data replication and failover software

**Vaulting Services**—Real-time or near-real-time, host-independent mirroring of critical data between source and target storage systems

**Records Management: Archiving For Messaging**—Cost-effective, compliance-oriented assistance for storing and managing email throughout a user-defined lifecycle

*Monitoring Services—Around-the-clock performance and availability tracking*

**Device Monitoring**—Basic availability monitoring for devices and services using standard Internet protocols

**Platform Monitoring**—Performance monitoring on the health of a server operating environment

**Database Monitoring**—Installation, configuration and management of database management systems

**Web Monitoring**—Status alerts of URLs and portals, in addition to performance and response time tracking

*Network services—Fast, reliable, on-demand access to a protocol-independent network*

**Net ReDirect**—On-demand circuit access to any SunGard facility with bandwidths of DS-1 to Gigabit Ethernet

**Web ReDirect**—Private Internet eXchange (PIX) Transit connections to ISPs

**10/100 LAN Bridging**—System connections among SunGard recovery facilities as if they were directly connected through a hub or a switch

**Managed CPE**—Router/circuit monitoring and management of customer premise equipment (CPE)

**Managed Internet**—1-100 mbps burstable Internet access for redundant Internet connectivity

**V\*Net**—Access through SunGard for all customers to the major telecommunications providers over a single connection

**Managed Load Balancing**—Management and troubleshooting of customers' load-balancing equipment

*Email Management Services—Objective advice on email availability issues*

**Email Availability Service**—Enablement of seamless and transparent email activity in the event of an outage

**Archiving Service for Email**—Effective management of inactive email, with special consideration for corporate policies and regulations

**Email Replication Service**—Use of real-time data replication and failover to ensure that active emails are immediately available following an outage

*Software Tools—Next-generation software for information availability*

**SunGard Paragon**—Centralized oversight of decentralized process ownership that captures the intellectual capital of hundreds of consultants and thousands of engagements

*Business Continuity Services—Expert assistance in developing the processes and procedures for business continuance*

**Systems Recovery**—Traditional hot-site recovery services

**End-User/Work Group Recovery**—An aggregate solution to protect critical business functions

**Mobile Recovery**—A flexible mobile solution that provides the need for an environmentally controlled alternate workspace

## About SunGard Availability Services

From initial assessments and plan development through execution and ongoing management, **SunGard Availability Services** offers a one-stop source for helping organizations integrate risk management and incident response into their information availability plans. SunGard Availability Services delivers solutions to support information availability—keeping people and information connected no matter what. Information availability requires not only technology, but also people, processes and physical infrastructure. Therefore, SunGard offers a full continuum of **managed IT**, **professional** and **business continuity services**:

- SunGard's **managed IT** services provide a secure, reliable environment to host mission-critical systems and applications. Offering a full portfolio of outsourcing and support services, SunGard gives clients the option of point or turnkey solutions.
- From assessing needs to designing solutions, our **professional services** help clients address availability challenges. We deliver information security, high availability and business continuity services, as well as services designed to help clients address regulatory requirements. We also deliver SunGard Paragon™, a next-generation information availability software tool.
- With one of the most extensive infrastructures in the industry, SunGard also delivers **business continuity services**. From traditional hotsites to leading-edge high availability solutions, our offerings enable clients to meet availability requirements.

SunGard Availability Services is an operating group of SunGard (NYSE:SDS), member of the S&P 500. With more than 25 years of experience helping organizations ensure information availability, we are uniquely positioned to provide vendor-independent recommendations and solutions. For more details on our services, visit our website at [www.availability.sungard.com](http://www.availability.sungard.com) or call 1-800-434-0002.