MessageSolution™

Enterprise Archiving, eDiscovery, Migration

Regulatory Compliance Management

MessageSolution Information Archiving & eDiscovery Platform

MessageSolution™
Enterprise Archiving, eDiscovery, Migration

Regulatory Compliance Management

MessageSolution Information Archiving & eDiscovery Platform

Table of Contents

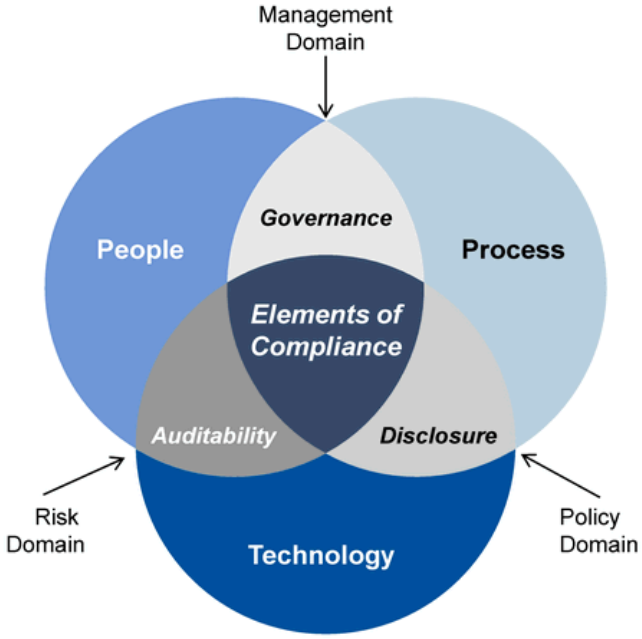
Chapter 1: Introduction

Throughout the world, there are strict regulations laid out by industries and all levels of government to regulate the protection and lifecycle of Electronically Stored Information (ESI). Most regulations require organizations to invest a combination of financial, technical and human resources to achieve compliance. According to Gardner Research, more than $6 billion was spent on compliance with Sarbanes-Oxley alone.

MessageSolution provides a turnkey solution that allows each organization to customize information archiving, retention and privacy policies to achieve comprehensive compliance. Multi-tiered policy capabilities also allow organizations to balance record retention with data storage optimization and mitigating unnecessary legal risk.

The Critical Elements of Compliance

There are three critical elements of regulatory compliance with overlapping relationships: process, people and technology. Together, these form the basis of all compliance efforts. These, in turn, overlap with governance structures, disclosure and auditability.



The central circle indicates other areas of intersection — specifically:

- The management domain occurs at the intersection of people, governance and process.
- The policy domain occurs at the intersection of technology, disclosure and process.
- The risk domain occurs at the intersection of people, auditability and technology.

John A. Wheeler, French Caldwell "*Understanding the Components of Compliance*" 24 July 2012 ID:G00234045. Gartner, Inc.

Chapter 2: Regulatory Compliance Regulations by Industry

Finance		
Registered Investment Advisor	Investment Advisors Act SEC Rule 204-2	Relevant data must be kept for no less than 5 years
Internal Auditor	Sarbanes-Oxley (SOX) section 802	Retain relevant data for no less than 7 years
Internal Auditor	IRS (IRC/FICA) 26 CFR 31.6001	Retain relevant data for 4 years after tax due date or date paid, whichever is later. Data related to a claim must be kept for 4 years after filing date
Bank	Gramm-Leach Bliley Act (GLBA)	Ensure confidentiality of customer financial information
Hedge Fund	SEC Rule 203(b)(3)-2	No less than 5 years
Broker Dealers	SEC 17a-4	Surveillance
Healthcare		
Health Insurance	The Health Insurance Portability and Accountability Act (HIPAA)	Retain and protect patient information for 6 years or 2 years after patient passing
Hospitals	The Health Insurance Portability and Accountability Act (HIPAA)	Retain and protect patient information for 6 years or 2 years after patient passing
Medical Records	DHHS (Medicare) 42 CFR 482.24,26,52	Medical records must be kept for 5 years after the last entry or change unless required to retain longer by state law
Education		
Education Records	State Law Requirements	Some state laws require educational records to be kept for a set period of time
Educational Records	DOEd (FERPA) 34 CFR 99.32	Data relating to transactions FERPA transactions must be kept as long as the student record is maintained

Financial Aid	DOEd 34 CFR 74.53 34 CFR 80.42	Records of education grants and other financial awards must be kept for 3 years after submission of final report
Business		
Employment	EEOC (ADA et al) 29 CFR 1602.14,21,28,40,49	Employment records for be kept for 1-2 years
Records	DOL (FLSA) 29 CFR 516.5	Payroll records, contracts or collective bargaining agreements, and other information must be kept for 3years
Business Records	DOL (FLSA) 29 CFR 516.6	Basic business records must be retained for 2 years
Welfare and Pension Records	DOL (WPPDA) 20 CFR 10.410	Reports under the Welfare and Pensions Plan Disclosure Act must be kept for 5 years
Welfare and Pension Records	DOL (ERISA). 29 CFR 4007.10	Employment records relating to pension and benefit plans must be kept for 6 years
Safety Records	DOL (OSHA) 29 CFR 1910.1020	Data relating to employee exposure or safety records must be retained for 30 years
Research & Intellectual Property		
Contract or Grant-Funded Research	Local Policies based on NIH, EPA GLP, FDA GLP, FDA GCP et al	Records associated with contract or grant-funded research must generally be kept for 3-5 years
Animal Research	NIH, USDA, PHS	Animal Research Records must be kept for 3 years after end of activity
Research Data	OMB-A110.53 2CFR 215	Research data must be kept for 3 years after research or audit is complete, whichever is later
Environmental Research	EPA (GCP/GLP) 21 CFR 160.195	Records relating to EPA-controlled research must be kept for 2-5 years
Biology Research	FDA (GCP/GLP) 21 CFR 58.195 21 CFR 312.57,62 21 CFR 812.140	Records relating to FDA-controlled research must be kept for 2-5 years
National Science Foundation Grant Research	NSF Grant Policy NSF 02151 sect. 350a	All records and supporting documentation relating to a NSF grant must be kept for 3 years after the award period, report submission or end of related proceedings
Patents	USPTO 37 CFR	There are no specified regulations, but best practice is patent term plus any extensions

Chapter 3: Regulatory Compliance Regulations by Country

USA		
Civil Procedure	FRCP	Rule 34(a) was amended to include discovery of data compilations Rule 26. Duty to Disclose; General Provisions Governing Discovery eDiscovery Federal Rules 16(b)
General Business	FRCP	26(f): Meet and Confer on Data Sources: April 29, 2015 Supreme Court Rule 37(f) provides safe harbor (protection against sanctions) Legal Hold
Canada		

**Financial Services
HealthCare
Public Sector**
	Mutual Fund Dealers Association (MFDA)
	PIPEDA29.7
		• Mutual Fund Dealers Association (MFDA)
		  • Mutual Fund Dealers Association (MFDA)
		  • PIPEDA

EU		
EU Retail Organizations, & those Doing Business with end users	General Data Protection Regulation (GDPR)	Art. 85 GDPR Processing and freedom of expression and information Chapter 3 (Art. 12 – 23) Rights of the data subject https://gdpr-info.eu/chapter-3/
Educational Records	DOEd (FERPA) 34 CFR 99.32	Data relating to transactions FERPA transactions must be kept as long as the student record is maintained
Financial Aid	DOEd 34 CFR 74.53 34 CFR 80.42	Records of education grants and other financial awards must be kept for 3 years after submission of final report

UK		
Field of Financial Controller and Processor (Applied to all organizations that control and process the personal data in EU)	The Data Protection Act 1998 (c 29) is a United Kingdom Act of Parliament (DPA)	Designed to protect personal data stored on computers or in an organized paper filing system Any data processing transfer activity involving sensitive data, data on creditworthiness and data relating to criminal or administrative offences is subject, in principle, to prior approval by the DPA
Information Security Management	British Standards Institution	BS 4783, BS 7799/ISO 17799, BS ISO 15489-1
Risk Management	British Standards Institution	**BS 7799 Part 3** was published in 2005, covering risk analysis and management. It aligns with ISO/IEC 27001.
Records	DOL (FLSA) 29 CFR 516.5	Payroll records, contracts or collective bargaining agreements, and other information must be kept for 3 years
Public Sector	Freedom of Information Act 2000	An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and for connected purposes
Business Records	DOL (FLSA) 29 CFR 516.6	Basic business records must be retained for 2 years
Welfare and Pension Records	DOL (WPPDA) 20 CFR 10.410	Reports under the Welfare and Pensions Plan Disclosure Act must be kept for 5 years
Welfare and Pension Records	DOL (ERISA). 29 CFR 4007.10	Employment records relating to pension and benefit plans must be kept for 6 years
Safety Records	DOL (OSHA) 29 CFR 1910.1020	Data relating to employee exposure or safety records must be retained for 30 years
Germany		
Contract or Grant-Funded Research	Local Policies based on NIH, EPA GLP, FDA GLP, FDA GCP et al	Records associated with contract or grant-funded research must generally be kept for 3-5 years
Tax Records	German Principles of Data Access and the Auditability of Digital	The German Tax Code controls the requirements for tax-relevant emails. Pursuant to the Tax Code, tax-

	Records (GDPdU), a set of administrative instructions	relevant emails must be retained for either six or 10 years
Animal Research	NIH, USDA, PH	Animal Research Records must be kept for 3 years after end of activity

For more information, please visit us at www.MessageSolution.com

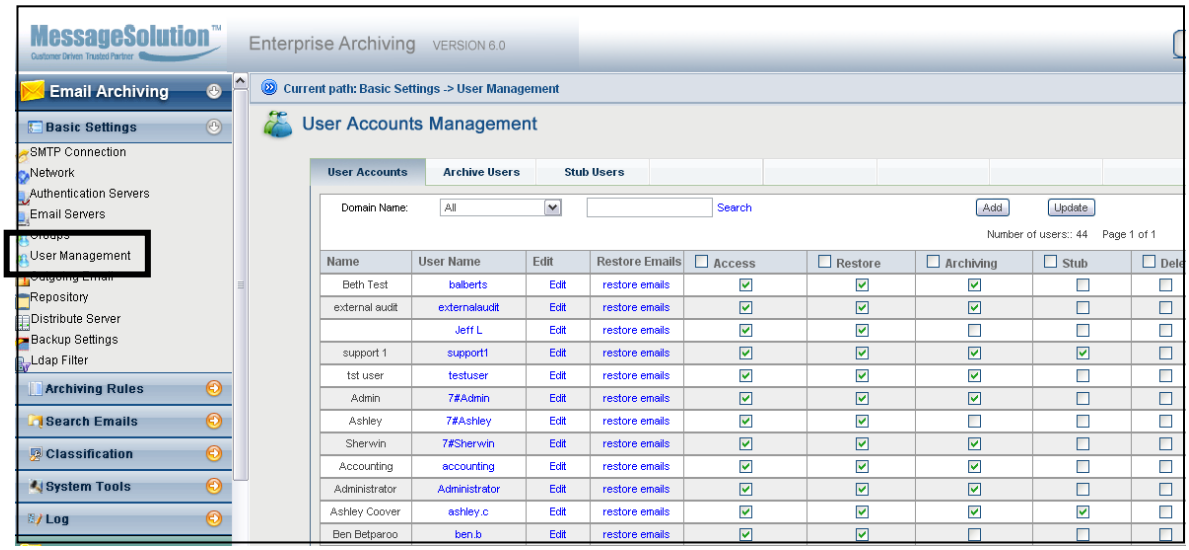
Chapter 4: Archiving for Regulatory Compliance
with MessageSolution Enterprise Information Archive

Real-Time or Journal Archiving

One almost universal aspect of compliance, no matter what regulations your company falls under, is capture and retention of all relevant emails and attachments. Organizations using MessageSolution Enterprise Email Archive for compliance utilize our real-time, or journal, archiving feature. The MessageSolution archiving system connects to your mail server's existing journal mailbox (for Exchange, Domino, Lotus Notes, Kerio, Imail, Zimbra etc.) and intercepts every incoming, outgoing or internal piece of email and immediately archives it before it can be deleted or altered in any way.

Multi-Tiered Access Permissions with Granular Feature Control

Many compliance regulations specifically require limiting internal access to certain electronic information, usually confidential medical records, financial statements and other highly private information. The archiving system allows the administrator to enact multi-tiered access permissions for individual users or user groups based on things like department or clearance level. Features like archive access, archiving, stubbing and delete functionality and data restoring capabilities can all be independently enabled for each user or user group.



EEA fully integrates with email clients directory services (like Active Directory, Domino Directory, GroupWise eDirectory, etc). Among other perks, this allows the system administrator to import all users/user groups directly from the email directory service.

Possible email archive access capabilities include:

Administrator(s): Unlimited access capabilities, Auditor/Legal configuration access, delete capabilities

User(s): Search, retrieve, restore, and configurable delete capabilities for their personal archive and for designated custodian archives

Policy-Driven Information Archiving

We know that effective policies are the backbone of compliance efforts, which is why Enterprise Email Archive's archiving rules are based on administrator-determined policies. Enterprise Email Archive allows you to create an unlimited amount of archiving policies by specifying email retention periods, storage repositories, filtration rules, size of messages to stub, stubbing of email contents and/or attachments, and other parameters. Apply specific policies to entire geographic locations, departments, or teams, all the way down to the individual user level. Set multiple repositories to manage storage hierarchically.

Automated Email Management

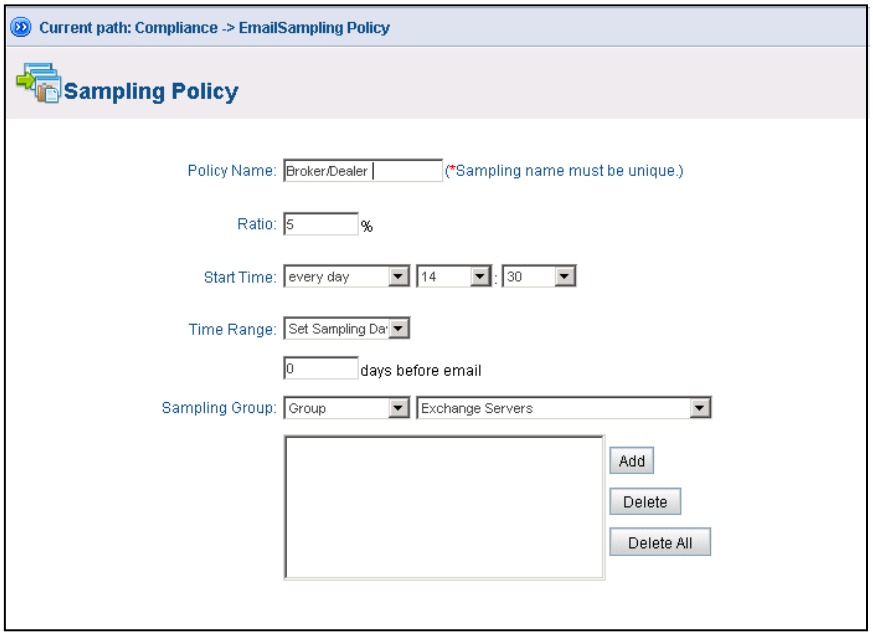
Unless users adhere to their company's email use guidelines, even the best compliance-geared policy is ineffective. Enterprise Email Archive gives management a tool to enforce email use policies automatically. IT and non-IT employees will no longer be responsible for managing email inbox storage, giving employees back anywhere from minutes to hours every week. With Enterprise Email Archive, management will not need to impose mailbox quotas; users, in turn, will have no need to create desktop archive files (PST, NSF files, etc.).

Auditor/Legal Access

Administrators may also configure Auditor/Legal Access for third party auditors or internal legal console as needed. With Auditor/Legal Access, auditors or attorneys will be able to independently search and access selected custodians' mailboxes.

Random Sampling

When an audit is performed, random sampling is typically used in lieu of overseeing every piece of archived mail. With MessageSolution Random Sampling feature, auditors can set granular parameters for the sample. While mostly used by brokers and dealers under the FCC, random sampling is to monitor insider trading and information control.



Email Archive Monitoring Reports

Enterprise Email Archive tracks archiving processes and user activity within the archive, maintaining multiple reports:

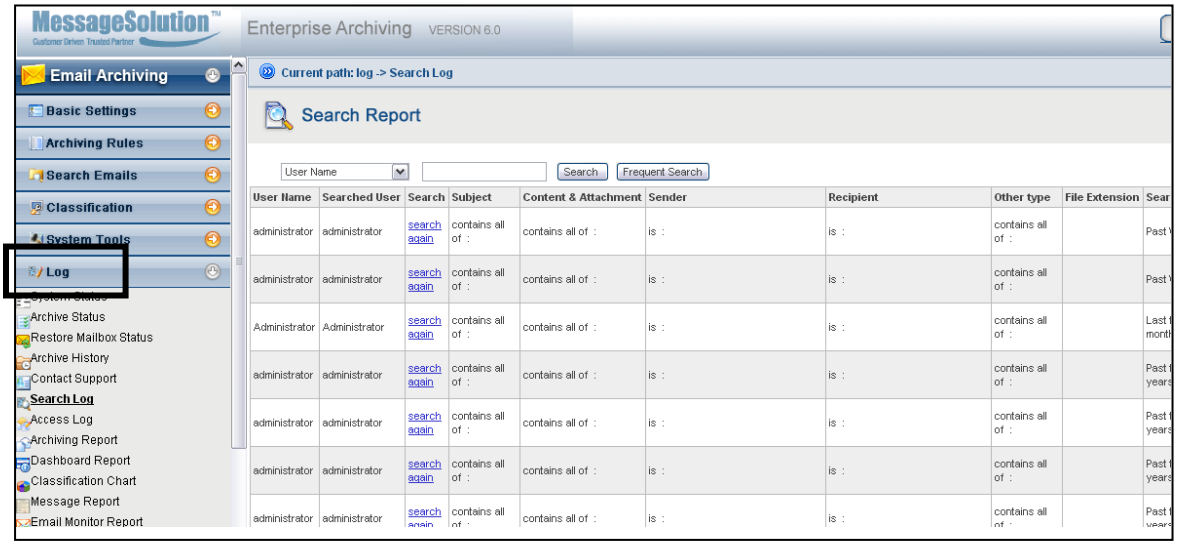
Search Report -- details who searched and when; terms used to search; number of queries returned

Access Report -- monitors who accessed the archive, what action was taken; actions include view, download, restore, log in, etc.

Archiving Report -- which email boxes are being archived; how many messages are in the email box; size user is occupying in archive storage repository

Status Reports -- reflect the current state of the archiving application and system status. User, actions, IP addresses, subject, sender, and inquiries are some of the information available from the reports, which help provide a picture of the type of usage the archive is put to.

Reports can be exported and used in combination with other reports and reporting tools as part of litigation support or performance tuning.



Bottom Line: Streamline Infrastructure, Improve Operations

With all your organization's data centralized in Enterprise Email Archive's collection folders, you can refine email data to further analysis and distribution. With mailbox quotas no longer required and each user capable of searching his/her own archive from any location, the time consuming task of managing one's inbox is eliminated, allowing staff to focus on the business at hand. Enterprise Email Archive relieves IT staff of hours of manually managing storage, all while ensuring total compliance.

Chapter 5: Commonly Encountered Global and Federal Regulations Dealing with Electronic Stored Information (ESI) Management & Retention

Code of Federal Regulations (CFR)

The Code of Federal Regulations (CFR) is the codification of the general and permanent rules and regulations (sometimes called administrative law) published in the Federal Register by the executive departments and agencies of the federal government of the United States. Many titles of the regulations deal with the handling and accessibility of electronic communications and documents as well as internal data management requirements.

http://www.archives.gov/federal-register/cfr/

The Fair Labor Standards Act (FLSA)

The Fair Labor Standards Act 1938 (FLSA), also referred to as the Wages and Hours Bill, is a federal statute of the United States dedicated to regulating and enforcing labor standard in the job market. It requires that employment records such as payroll records, contracts, etc be retained.

http://www.dol.gov/compliance/laws/comp-flsa.htm#.UKWJ_eTWK8o

Gramm-Leach Bliley Act (GLBA)

The Gramm–Leach–Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999, mandates that both internal and external safeguards and limited access be applied to electronic records and communications to protect client confidentiality.

http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is designed to protect health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

http://www.hipaa.com/

Investment Advisors Act of 1940 (IAA)

The Investment Advisers Act (IAA) was passed in 1940 in order to monitor those who, for a fee, advise people, pension funds, and institutions on investment matters. It requires that all electronic communications, documents and records relating to investment advisory activities be available for audit by the SEC or state regulatory agency and for no less than 5 years.

http://www.sec.gov/about/laws/iaa40.pdf

US Occupational Safety and Health Administration (OSHA)

The United States Occupational Safety and Health Administration (OSHA) is an agency of the United States Department of Labor dedicated to assuring safe and healthful working conditions for working men and women by setting and enforcing standards and by providing training, outreach, education and assistance. OSHA regulates the retention and management of all safety records and incident reports.

http://www.osha.gov/

Sarbanes-Oxley Act (SOX)

T he Sarbanes–Oxley Act of 2002, also known as the 'Public Company Accounting Reform and Investor Protection Act' and 'Corporate and Auditing Accountability and Responsibility Act' is a United States federal law that sets new or enhanced standards for all U.S. public company boards, management and public accounting firms. It deals with regulatory audits based off unalterable records. It also mandates internal controls and other regulations designed to mainstream electronic record management.

http://uscode.house.gov/download/pls/15C98.txt.

Securities Exchange Commission (SEC)

The Securities Exchange Commission (SEC) is a federal agency which holds primary responsibility for enforcing the federal securities laws and regulating the securities industry, the nation's stock and options exchanges, and other electronic securities markets in the USA. SEC Rules regulate topics from quarterly and bi-annual audits to data lifecycle management.

http://www.sec.gov/rules/final.shtml

US Department of Education (DOE)

The US Department of Education (DOE) regulations the management of electronic communications and records that relate to any monetary student transactions relating all scholarships and grants. It also regulates compliance with the Family Educational Rights and Privacy Act (FERPA) relating to the confidentiality of student information.

http://www.ed.gov/

US Department of Health and Human Services (DHHS)

The US Department of Health and Human Services (HHS) regulates the retention and management of electronic medical records and patient confidentiality.

http://www.hhs.gov/

US Department of Labor (DOL)

The purpose of the US Department of Labor is to foster, promote, and develop the welfare of the wage earners, job seekers, and retirees of the United States; improve working conditions; advance opportunities for profitable employment; and assure work-related benefits and rights. It regulates the management and retention of employee records and submitted reports.

http://www.dol.gov/

US Equal Employment Opportunity Commission (EEOC)

The U.S. Equal Employment Opportunity Commission (EEOC) is a federal law enforcement agency that enforces laws against workplace discrimination. It regulates the retention and confidentiality of employment records and more.

http://www.eeoc.gov/

Chapter 6: About MessageSolution, Inc.

MessageSolution is an industry leader in enterprise-class information archiving and eDiscovery solutions for email, SharePoint, and file systems, supporting all hosted email platforms including Microsoft Office365, SharePoint Online and OneDrive. Available as enterprise on-premise, cloud and MSP-Hosted multi-tenant platforms, MessageSolution Enterprise Archive helps ensure regulatory compliance, handle eDiscovery requests and mitigate legal risk, manage data growth and optimize enterprise data management efficiency. An effective in-process data compression coupled with data de-duplication allows MessageSolution to save up to 75% of storage space and archive for 25,000+ users on each single server which leads the market with 5 or more times cost reduction on hardware requirement. MessageSolution offers a seamless platform for searching and accessing archived data. The solution is intuitive and easy for users at all company levels to utilize.

MessageSolution's team of dedicated professionals comes from a wide array of companies in Silicon Valley, California, including technology veterans from IBM and previous Sun Microsystems, as well as graduates of Stanford University. With more than 20 years of high tech experience, the MessageSolution team puts everyone's skills to work creating software to solve IT problems for enterprises in various industries across the world. Managed by a team of highly experienced Silicon Valley veterans, MessageSolution is positioned to lead the rapidly growing enterprise information archiving and eDiscovery markets.

MessageSolution is headquartered in Silicon Valley, California, with operations in North America, Europe, and mainland China, along with distribution channels in Europe, South Africa, Australia, and Asia Pacific. We are a growing independent software vendor dedicated to providing innovative email, file systems, SharePoint, Office365, and video archiving for compliance, electronic discovery, storage management, and mail cross-platform migrations.

External Sources

John Bace, Carol Rozwell, Joseph Feiman, Bill Kirwin "*Understanding the Costs of Compliance*". Gartner, Inc. <http://logic.stanford.edu/poem/externalpapers/understanding_the_costs_of_c_138098.pdf>

John A. Wheeler, French Caldwell "*Understanding the Components of Compliance*" 24 July 2012 ID:G00234045. Gartner, Inc. <http://my.gartner.com/portal/server.pt?open=512&objID=255&mode=2&PageID=2321871&resId=2091615&ref=QuickSearch&sthkw=regulatory+compliance>