

Most Commonly Asked Chief Compliance Officer (CCO) Questions and Issues

ZL TECHNOLOGIES, INC.
WHITE PAPER





Table of Contents

Introduction 2

Most Commonly Asked CCO Questions..... 2

Issue 1 2

Issue 2 3

Issue 3 3

Issue 4 4

Issue 5 5

Issue 6 5

Issue 7 6

Issue 8 7

Issue 9 8

Issue 10 9

Issue 11 10

The ZL Unified Archive 10

About ZL Technologies..... 13

Introduction

The email archiving for compliance space continues to grow and evolve at an almost-alarming rate. New regulations from regulatory bodies such as the SEC and NASD have spent the last few years aggressively fine-tuning their requirements and as a result, organizations, particularly in the financial sector, are having trouble keeping up.

Overall, the general idea that email archiving is something necessary has seeped into the hearts and minds of CEOs, but generally only a company’s Chief Compliance Officer (CCO) and Legal Counsel may truly be aware of what regulations impact the organization directly, what the requirements are, and that the benefits of having (and paying for) an email archiving solution for compliance far outweigh the penalties of not.

Unfortunately, email archiving for compliance is in essence a sunk cost, i.e. there is no real immediate ROI (Return on Investment) as for broker dealers, hedge funds etc., it’s either have it, or go to jail and be heavily fined should an audit or review come up. Cases such as those involving *Enron*, *WorldCom* and *Martha Stewart* have made sure of that. Paranoia is running rampant, and more often than not, organizations feel pressured to deploy a solution to make them feel safe just because they have it, without fully researching if it a) is truly compliant, and b) will continue to meet their needs as the organization continues to grow and expand. CCOs are constantly battling with company CEOs, legal departments and IT to determine exactly what it is they need, what regulations affect them today and will do so tomorrow, and so on, and oftentimes issues arise that appear easy to solve at first glance, but have sever repercussions if not tackled correctly.

ZL Technologies (ZL) has accumulated data from over 500 companies in regulated industries, including financial and healthcare. Additional information was also gleaned from compliance officers and SEC personnel at various compliance conferences.

Most Commonly Asked Chief Compliance Officer (CCO) Questions

The following are the most commonly asked CCO questions and issues, and the responses to them, as compiled by ZL Technologies, after three years of feedback and insight in the email archival space.

- 1. My CEO doesn’t think that archiving corporate email is important for regulatory compliance, nor does he take personal responsibility for compliance.**

Response:

- a. The SEC, NASD Investment Advisors Act, HIPAA and Sarbanes-Oxley all specifically recognize email as a business record. In fact, 70% of all important business



content is in, or accessible via, email. CEO's can no longer ignore the requirements, or the penalties, both to themselves and to their company.

For example:

NASD Rule 3013 went into effect Dec 1, 2004 and requires both the CEO AND CCO to certify that all compliance processes have been defined, tested, and meet NASD standards. The penalties include heavy fines and jail time for both parties. Under Sarbanes-Oxley, the CEO's of *Enron*, *Tyco* and *WorldCom* are poster-children for corporate malfeasance and the ensuing criminal and civil penalties.

2. My CEO wants to spend as little money as possible on regulatory compliance

Response:

- a. Compliance solutions for archiving are not generally perceived to have an immediate or obvious ROI (Return on Investment). However, as a result of frequent audits, subpoenas, and stringent laws, in the compliance world, ROI has taken on a whole new meaning - "Risk of Incarceration." While financial firms have a legitimate reason to feel coerced into purchasing a compliance/email archiving solution, the initial perceived savings in purchasing a cheap solution that is not truly compliant would be wiped out by the heavy fines and possible jail time. "No ROI" becomes a benefit, rather than a detriment to a compliance solution.

For example:

In March'04, the SEC fined Bank of America for securities fraud charges because Bank of America traders were receiving inside information from internal analysts, and using it prior to public release to time the market. BofA agreed to pay a total of \$375 million. According to the SEC, the settlement was a new benchmark in mutual fund market timing and late trading.

The SEC also found that Bank of America Securities failed repeatedly to promptly furnish documents including internal emails requested by the staff as part of the investigation. BAS has agreed to a censure and a \$10 million civil penalty.

3. We are already archiving in Microsoft Exchange/Lotus Notes, isn't that enough?

Response:

- a. The SEC does not consider simply storing messages in Exchange or Notes to be compliant due to the ease of alteration or deletion of email messages in these email server systems – by savvy administrators or email users. Also, some versions of Exchange and Notes do not properly record all types of email messages required for compliance, including key types such as Blind Carbon Copies (BCCs) and group list aliases. Complete electronic records must



include these in order to be compliant, and the situation becomes aggravated if during cross-company corroboration, another company produces such email and yours does not.

- b. One of the key requirements of archiving for compliance is not just to store messages, but to be able to search quickly and comprehensively in response to an audit or subpoena. Searches typically involve not just basic header information (to, from, date) but also various key words and phrases, and whether these appear in the body, attachment, or even disclaimer of the email. Audits or subpoenas typically give companies very short time limits to produce requested communication. These days, the time frame granted by regulatory officers to produce emails can vary from 2 weeks down to only a few hours. Exchange and Notes search capabilities are extremely limited, lack depth and granularity, and are simply not up to the task.

4. The SEC auditors only come around every four years or so. I have plenty of time to deploy a solution and prepare for compliance.

Response:

- a. Companies will never know when SEC auditors are going to show up. The SEC Chairman has announced that the SEC is going to be more "preventative and anticipatory" in their audits, and no longer wait for cause. More and more companies have experienced frequent "spot checks" that often include email compliance.
- b. A compliance solution is also critical as companies will never know when they might be involved in a lawsuit unrelated to SEC or NASD auditing/compliance, such as a sexual harassment case. A proper compliance solution will lower search and discovery costs, and help minimize exposure.

For example:

ZL Technologies' "Attorney/Client Privilege" features enable CCOs and compliance auditors to flag and exclude messages between lawyers and clients from a found set so that only a log citing the message header and subject of the privileged mails need be turned in for review. ZL also features "Compound Search" to search on multiple fields (date range, to/from, body, attachment etc.), and "Full Text Indexing" which can search on any word in a message to pull up the smallest possible found set based on the criteria.

In the event of a lawsuit or subpoena, a weak search engine will return a far larger result set, and an index based only on key words, may not return a found set at all if the search string wasn't pre keyed in the index. Either weakness in search capabilities exposes the company to further discovery and liability.



5. I don't want the administration headaches of an in-house enterprise archiving solution.

Response:

- a. Deployment is 80% of administration for ANY solution; a hosted solution won't even avoid the remaining 20% of the administration if the solution requires an onsite message agent, which will still require management and administration. Standard compliance tasks (post-review, flagging, search, reporting etc.) will need to be handled in-house regardless of whether the solution is hosted or enterprise.

- b. There are always trade-offs between a hosted and an enterprise solution. The downside of a hosted solution is the lack of control of corporate data. In an enterprise environment, if the SEC or a law enforcement agency wants to investigate or subpoena company data, they must serve the corporation with notice. In a hosted environment, they can go directly to the hosted provider who IS LEGALLY NOT ALLOWED TO TELL or notify the regulated company that data has been searched and compromised. (See USA Patriot Act <http://www.epic.org/privacy/terrorism/hr3162.html>)

For example:

Should you be using a hosted solution that happens to house data for an Islamic charity, if the FBI or any other law enforcement agency needs to get access to that data, they can demand that all the information housed by the hosted provider be handed over to them. You will never be notified that your data has been compromised.

6. Having my compliance solution hosted seems so much more cost-effective.

Response:

- a. Be wary of incremental fees. Hosted solutions charge additional monthly fees for storage over a minimum initial amount.

For example:

A good analogy would be with car leases – car leases are based on a monthly fee, plus a per mile penalty if the car is driven over a pre-defined mileage quota. Hosted solutions price based on the number of mailboxes, plus a monthly fee for storage over 4GB. With minimum retention periods of three years, fees of \$20 per extra GB per month can add up to thousands of dollars annually in unbudgeted overhead cost.

- b. In order to meet compliance rules, companies must keep a copy of all corporate communications data in-house. Hosted providers charge a fee for companies to receive copies of their own data.



For example:

Hosted providers can charge \$50 per DVD per month for a copy your own data. DVDs hold only 4 GB of data which must include the archive, index and search engine.. Depending on the amount of data and number of employees, the cost to keep your own data can run in the thousands of dollars a year.

- c. If the hosted provider goes offline unexpectedly, your ability to send and receive mail will be offline as well, otherwise all emails sent during the outage would not be archived. With the added external hop in your mail chain, scaling issues and bottlenecks at the hosted site will also lead to delays in delivery and receipt of your mail. This is regardless of whether your company has a mail server in-house.
- d. The SEC turnaround times for responding to audit requests have shortened from a matter of days to a matter of hours. Companies today are completely at the mercy of your hosted provider's additional response times.
- e. Regardless of the size of an enterprise, when utilizing a hosted solution, you will no longer have control over bandwidth. Companies trying to access or review messages at the same time other hosted customers are accessing the system, will be subject to long lag times and bottlenecks. ZL has research data indicating 5-8 second-lag times to pull up a single message for review. If compliance officers are reviewing 1,000 messages a week, they will waste an additional 150 minutes, or 2½ hours, downloading the data in addition to the time required to actually perform review tasks.

7. We don't have an internal IT department so it is still more effective to purchase a hosted solution. They say their security measures are just as good as our own.

Response:

- a. There are always trade-offs between a hosted and an enterprise solution. The downside of a hosted solution is the lack of control of corporate data. In an enterprise environment, if the SEC or a law enforcement agency wants to investigate or subpoena company data, they must serve the corporation with notice. In a hosted environment, they can go directly to the hosted provider who IS LEGALLY NOT ALLOWED TO TELL or notify the regulated company that data has been searched and compromised.
- b. In a hosted environment, your company's corporate data is co-mingled with other hosted customers on the storage array. When the SEC and law enforcement agencies subpoena another company's data on any array, ALL data on that same array (including yours) will be swept in the search and the hosted provider is legally prohibited from



informing you. You will never know if your data has been viewed, and sensitive information compromised.

- c. Hosted email archiving can create a PR nightmare that may not have existed if corporate data had been kept in-house. State-specific regulations such as the California Encryption Act (SB-1386) require that companies, which hold the personal data of a California resident (customer or employee), must notify those residents immediately after their data has been breached, or believe to have been compromised.
 - Even if your company is not normally subject to such a state-specific law, there is no way of knowing whether your company's data is co-mingled with the data of a company who is, which makes the hosted provider subject to SB-1386.
 - The Law requires that all California residents with potentially compromised data be immediately notified. If not directly, then by means of the media (print, TV, Web etc.). A hosted provider would not only be required to announce its breach of security but also the breach of data of all of its customers (your name here).

8. Our lawyers have reviewed documentation from your competitors and said that they are adequate for our needs. So why should we go with your solution, which seems like overkill?

Response:

- a. CCOs and CEOs must carefully review the regulations specific to their company, whether it is a broker dealer, investment advisor, or hedge fund etc. All regulations for the financial industry are modeled after the most rigid, which is SEC 17a-4 for broker dealers. The lesser regulations are rapidly being fine-tuned, and following in the footsteps of 17a-4. Many solutions on the market today only meet the bare minimum requirements for the lesser compliance regulations, and will be unable to keep up with the regulations as they change. You have to archive data for a period of years; it does not make sense to purchase a solution that will not meet your needs for the entire length of the requirement.
 - It is far easier to purchase a solution that meets your needs both today and down the road, and implement the long-term features when needed. The expensive alternative is to purchase either an entirely new solution to meet the regulatory changes, or to purchase additional point-solutions that require additional hardware, software and integration. Data archived on old



solutions using proprietary software will either have to be maintained on a legacy system, or have to be further migrated for compliance, incurring additional and unnecessary fees.

- b. Most competitive solutions on the market today have major architectural holes which prevent them from being providing a truly compliant solution. They either only “journal” or sit at the gateway.
 - Competitive solutions that only journal are easy to circumvent because they cannot capture BCCs and will cause compliance headaches due to their inability to recognize the individual recipients in a group list.
 - Gateway solutions are not able to capture internal-to-internal mail. Such messages are critical both for SEC (including Investment Advisors’ Act) compliance and are the most requested data for subpoenas and lawsuits (legal discovery).
 - Only a solution that can handle both journaling and gateway capture is truly compliant.

9. I just want to meet the minimum requirements for compliance now, and will consider upgrading down the road.

Response:

- a. Waiting a year to implement a robust solution is playing with fire. Most compliance archival solutions store corporate mail in a proprietary format which locks you in to their solution for the long-term, or will incur very high fees to migrate data to a future archival solution. A rigid and lesser-quality solution will be unable to move with the times, and keep up with changing regulations.
 - Choosing a cheaper, more inflexible solution leads to either paying large migration fees, or having the additional headache of maintaining a separate standalone archive for the old solution. This will be in addition to the cost of any future implementation of a more robust compliance solution.
- b. It is a given that corporate messaging infrastructure will continue to evolve, including upgrading hardware, OS and mail servers. Choosing a solution that locks your infrastructure into a limited number of currently available architecture invites obsolescence and can have huge cost consequences down the road.



- ZL's Unified Archive is 100% server-side Java-based, and completely hardware, software, and OS-agnostic. ZL utilizes open standards, including storing mail in MIME format (the original email format), which enables ZL to seamlessly fit into any existing mail infrastructure, including environments running mixed platforms (i.e. Exchange and Lotus mail servers, or Windows and Linux OS, and AIX platform etc.). Such flexibility future-proofs corporate architecture, and allows the company, not the archive solution to dictate their technology roadmap.
- Also, in a world of mergers and acquisitions, it is entirely possible that corporate infrastructure could change into an environment of multiple OS, mail servers or both. Many large organizations such as the Fortune 100 companies have purposely segmented their messaging architecture, and specifically chosen to run multiple email environments. (Example: Lotus Notes for Executives and IT, and Exchange for Sales and Marketing). Only ZL can run and maintain a single archive in a mixed environment.
- MNCs traded on a US stock exchange are required to archive all email, regardless of location and language in which business is conducted. A compliance solution with double-byte language capabilities is necessary for any company who conducts business in any of the Asian languages, including Chinese, Japanese, Korean etc, and wants one corporate archive, rather than a myriad of separate archives.

10. We have a 90-day deletion policy, specifically because we do not want the liability of an archive.

Response:

- a. Sarbanes-Oxley, which has three-year retention policies for corporate data, applies not only to public companies, but also to private companies that could at any time be acquired or go public. In short, no company is immune from potential liability under Sarbanes-Oxley. Section 802 of Sarbanes-Oxley mandates 20 years jail time for deleting email relevant to a current or future litigation. The only way to meet Section 802 is to archive all email for the required three-year retention period.
- b. Email is considered the “smoking gun” for search and discovery of relevant data for lawsuits. One in every five U.S companies has had employee emails subpoenaed for a litigious claim or regulatory investigation (Time Magazine, 2004), and the costs to produce the mails when a corporate archive doesn't exist are huge, and borne by the defendant.



For example:

In the case of Zubulake v. UBS Warburg, 1500 emails were admitted into evidence. The cost of search and discovery to recover the mail from 77 backup tapes was borne by the defendant, at \$4,000 per tape. UBS Warburg spent \$240,000 for document production and document litigation alone. In the 1999 case of Linnen vs. A.H. Robbins, recovery of internal mails for 15 users from backup tapes cost more than \$1 million, or over \$73,000 per mailbox.

- c. Just because a company itself no longer possesses a sent or received email message does not mean that the data no longer exists in the archives of the recipient. It is far better to know “where the bodies are buried” for purposes of damage control.

For example:

During their Department of Justice anti-monopoly investigation, Bill Gates testified before Congress that Microsoft never had a policy to destroy their competitor Netscape. Congressional investigators produced an old email Gates had authored (but didn't know still existed) detailing the policy he'd just denied.

11. Your product looks more tailored to meet the needs of the financial industry, than to mine in healthcare.

Response:

- a. Companies subject to HIPAA are not only required to archive records for 6+ years, they are also required to secure the data both in transit and at rest. There is a danger of having separate point solutions to encrypt and archive corporate data. Specifically, there is no way to search across the archive for encrypted content. In order to search an archive of encrypted data, it is necessary to have a product that integrates both the securing and the archiving of messages so that reviewers can search across the entire archive and produce required data regardless of whether it is encrypted or not.

The ZL Unified Archive

The ZL Unified Email Archive provides complete email archiving and management for companies using Lotus Notes/Domino, Microsoft Exchange, Novell Groupwise, Bloomberg, and others. The suite provides scalable storage of email data, email archiving, content management, regulatory compliance, lifecycle management, performance enhancement, hierarchical search and discovery, attachment management, and email continuity and disaster response.

The ZL Unified Archive (ZL UA) enables:

- Compliance with regulations - including complete email capture and email archiving, as well as pre and post-review capabilities



- Storage management and retention management
- Enhanced search and Legal Discovery
- Improved MS Exchange/Lotus Notes performance
- Email content management

ZL revolves around our customers' continued satisfaction and peace of mind. If your company needs to meet government compliance or best practices requirements, if your firm is concerned about email archiving for compliance or according to corporate policy, email security, business continuity; if your business needs to securely communicate between internal and external users, then ZL has the answer.

Comprehensive Solutions

ZL's suite of email archiving, secure messaging, and compliance solutions, are used by clients to extend compliance and to satisfy many of the regulatory requirements mandated by international and federal law. These include, compliance regulations under:

- Health Insurance Portability and Accountability Act (HIPAA)
- SEC Rule 17-CFR 270.17a-4 (SEC 17a-4), NASD 3010(d)/3110
- The Investment Advisors' Act (Rule 204-2)
- The Gramm-Leach-Bliley Act (GLBA)
- European Union Directive on the Protection of Personal Data (EU Directive)
- The US Patriot Act
- The Sarbanes-Oxley Act (SOX); US and Japan
- Basel Accords (Basel II)

Without the appropriate technology to manage and control your email or file data, organizations, their officers and executive directors are exposed. Breach of these laws can result in stiff fines and mandatory jail time. ZL's applications have been designed to specifically provide those private, governmental, and non-profit organizations that fall within the above regulations with the auditing, management, workflow process, and security technologies necessary to comply.

Absolute Archiving

In the past, archiving of email and attachments meant storing a few important emails as a possible future reference. Today, email archival is a critical part of regulatory compliance and business intelligence. Unlike other solutions that focus on one or two aspect of archiving, ZL combines all major aspects of archiving including: Email Data Archival and Compliance, Search and Retrieval, Mailstore Performance Enhancement, Gateway Control, Attachment Management, Email Storage Virtualization and Life Cycle Management, Global and User Level Email Content Management, and Email Continuity and Disaster Response. No other solution today provides such a comprehensive suite of functionalities on a single, integrated platform.



Scalable Security

In today's information-intensive business environments, the security of business information is paramount and through the ZL Secure option, ZL Applications can be deployed with complete, end-to-end security: secure access, authentication, audit trails, encrypted storage, secure delivery, etc. ZL encryption components are fully FIPS 140-1/FIPS 140-2 compliant: AES (FIPS 197), 3DES/DES (FIPS 46-3), and support international standard S/MIMEv3 and x.509v3 secure mail protocols as well as PKI standards XKMS (PKCS#7 and PKCS#12) for digital certificates and major certificate authorities.

Simple Deployment

IT groups can rapidly and cost-effectively deploy the ZL platform across the entire organization. Proven to scale from 25 to one million users, ZL's scalable platform enables an organization to instantly archive, secure, and control its email communications with a completely in-house solution. No outside service is required and the organization has 100% control of its critical and sensitive data. Today, one of ZL's customers, a Top 5 Global Bank, has the single largest repository for email archiving for compliance, not just mailbox management, with 25,000 users and growing.

Flexibility and Function

ZL's flexibility enables it to function as an internal server, as a gateway, or as both. High performance scaling and proven throughput for carrier-class volume enable ZL's solution to deploy where single or multiple locations in the network, wherever it is most needed. All ZL modules can be deployed from a single system or cluster of servers because it is a truly integrated solution, built from the ground up on a unified, highly scalable open standard platform.

Simple to Use

Senders and recipients have zero user training. ZL has spent over 200,000 man-hours engineering its server-based technologies to ensure the simplest, yet secure experience for recipients. Most major processes are fully automated such as retention policies, email data virtualization, user registration, password or key management, user authentication, encryption, housekeeping, etc. so that once set up, administrators never need to manage the system day to day.

Modular Design and Platform

Organizations today have immediate needs and a mandate to control costs. ZL's modular platform enables IT groups to acquire and deploy only those functions they needed today with no penalty or additional cost for adding optional modules tomorrow. This ensures the most cost effective solution for small, medium, and global organizations.



Deployment Options

The ZL Platform is 100% Java and designed to run in any network/firewall architecture (1, 2, multi-tiered) or back office environment. It is also ideally suited for enterprises focused on platform architectures such as J2EE or .NET and supports Web services through its ZDK API. As such, the ZL Platform is extremely flexible, running on all major operating systems, application servers, web servers, databases, and system platforms

About ZL Technologies Inc.

Established in 1999, ZL Technologies, Inc. (ZL) provides cutting-edge enterprise software solutions for email archiving, regulatory compliance, litigation support, corporate governance, content management, file archiving, and secure email. ZL's flagship product, the Unified Archive, offers comprehensive email and file archiving and management for companies using Lotus Notes/Domino, Microsoft Exchange, Bloomberg, and others. The suite provides a highly flexible framework that is fully scalable, enabling organizations of all sizes to meet legal discovery, compliance, and storage management requirements. With a proven track record and an impressive list of clients, including Walgreens, Bank of New York Mellon, Pacific Life, and Morgan Keegan, among other top global institutions, ZL has emerged as the premier provider of email archiving and compliance solutions. For more information, please visit www.ZLTI.com