

Kalypton[®]

Compliant communications and data management™

Compliant Electronic Records Management: Email Compliance

CONTACTS

For further information please contact:

Lars Davies
4 Corston Hollow
13 Woodlands Road
Redhill
Surrey
RH1 6BU
United Kingdom

Ian Walker
20 Hilfield
Yateley
Hampshire
GU46 6XP
United Kingdom

Mob: +44 (0) 7899 066367
Tel: +44 (0) 1737 764727

Fax: +44 (0) 1252 662129
Mob: +44 (0) 7768 354694
Tel: +44 (0) 1252 662129

All rights reserved. The information in this document is proprietary to Kalypton Limited. Without prior written approval of Kalypton Limited no part of this document may be reproduced or transmitted in any form or by any means, including but not limited to electronic, mechanical, photocopying or recording or stored in any retrieval system of whatever nature. Use of any copyright notice does not imply unrestricted public access to any part of this document. Kalypton® is a registered trade mark. Other trade marks are acknowledged as the property of their rightful owners.

This document does not in any way purport to be legal advice nor is it provided as such. The authors of the document and Kalypton Limited disclaim all liability for any inappropriate or improper use of the information contained in this document.

© 2004 Kalypton Limited. All rights reserved.

The right of L Davies and I Walker to be identified as the authors of this work has been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

DOCUMENT CONTROL

Owner	L J Davies	
Date	15 January 2004	
Version	X004/1.0	
Reviewed by		Date
L J Davies		19 February 2004
D I Walker		19 February 2004

Version History		
Version	Date	Details
X001/1.0	19 Feb 2004	First authorised version.

Abstract

This document covers the issues and requirements for achieving a compliant email solution.

Compliance is a massive topic. As a concept it seems simple; however for an organisation to achieve compliance is very complex. In essence, this requires the organisation, whilst conducting its day to day business, to obey all the relevant legal, regulatory, judicial, and corporate governance requirements, in addition to any applicable standards and codes of practice. These requirements are neither explicitly defined in any one place nor by any one body. It is for each organisation to determine what requirements it must comply with, and what actions should be taken to achieve compliance.

The objective of this document is to provide a clear introduction to the subject of email compliance. The document first highlights the rules and regulations that an email system must comply with. These rules and regulations are then used to derive both a set of requirements to be met and guidelines on the steps an organisation should take to meet them. The guidelines include which departments need to be included to fully determine the requirements and solution, where to start in defining individual requirements and what the components of a solution might be.

The document is aimed primarily at directors, both executive and non-executive. Directors have an obligation to understand the corporate governance issues that they face, including the legal issues and potential liabilities, both organisational and personal, surrounding the use of electronic mail and the use of electronic documents. The document is also aimed at those responsible for implementing a compliant system which includes the IT department, legal, human resources, risk management and security.

The document is applicable to all industries and contains specific pointers where appropriate for industries such as finance, telecoms, government, healthcare and pharmaceutical.

1 INTRODUCTION

Compliance does not just mean meeting the requirements of specific regulations such as Financial Services regulations. Compliance means meeting all legal and regulatory obligations that a commercial concern must face. In addition compliance means meeting judicial and corporate governance requirements. This comes from the fact that regulations, legislation, and other requirements of compliance cannot be understood in isolation from the legal framework within which they operate.

Email is just one, albeit a very significant component of doing business electronically. The issues extend to all forms of electronic communication and use of electronic records. This document concerns itself with email but the requirements can just as readily be applied to other forms of communication.

Before delving into the detail, it is worth standing back for a moment to understand the origins of the problem to be resolved. With these “first principles” in mind, it becomes much easier to understand how the various industry sectors have defined explicit regulations for the conduct of business, and particularly electronic business, within their sector.

The next section of this chapter provides a definition of what compliance means and the remainder addresses the background to electronic mail and its use in business.

1.1 Compliance

A compliant organisation is an organisation that obeys all the relevant legal, regulatory, judicial, and corporate governance requirements, in addition to any applicable standards and codes of practice. Compliance with a single regulation, where it is achieved in isolation from the other elements of compliance has little use as it may not guarantee compliance in its full sense. For example, if one regulation requires a retention period of 3 years, but another requires a retention period of 7 years, then the retention period must be set to 7 years. (Note, this may have implications on access rights under the former regulation.)

However, more fundamental to any regulation, is the fact that all regulations are subject to the jurisdiction and requirements of the courts, and it is these that must be met irrespective of the requirements of a specific regulation. This can lead to apparent anomalies, for example a regulation may seem to prohibit deletion of a record during the retention period but the courts have the power to order an incorrect record to be deleted or amended. Typically, retention periods required by the courts are longer than those defined by regulators as the courts require the record to be available until the need for that record expires under the statute of limitations. Regulators only define a retention period to cover the period that they have specific interest in the record.

Regulations tend to focus on which records need to be retained and for how long. Some go further, particular in the Pharmaceutical and Health Care sectors, and address the issues of integrity and authenticity of records in electronic form. This leads to the cornerstone of compliance, be it paper-based or electronic, which is demonstrating evidential weight for records. Evidential weight is covered more comprehensively in the next chapter; the concept that needs to be recognised as part of the discussion on compliance is that an organisation needs to

be in a position to demonstrate that the records it retains are the actual business records used and none has been added, changed or deleted.

Much of the information contained in this document, however, is relevant to the management of any type of electronic record. It would also be wrong to conclude that this document is only relevant to electronic records. In fact, the principles apply equally well to paper records and it is a common mistake to conclude otherwise. What is significant is that the ability to do business electronically throws up a range of technical issues that need to be addressed in order to give the same level of confidence, of evidential weight, to the record in electronic form. Compliance has always been a requirement for conducting business, but the advent of the computer age and recent high profile corporate scandals have raised the profile.

Compliance to put it simply is a cost of doing business.

1.2 The evolution of writing

Writing was developed in Babylonian times to record business transactions and tax receipts in order to provide strong evidence of a trade agreement. The transactions were recorded on clay tablets which provided data integrity and both sides had proof of the trade. In effect, the tablets provided non-repudiation.

Over time clay was replaced by papyrus, velum and today's paper and ink. This evolved to the printed and typewritten word, all the time making the process of recording information more efficient, whilst being able to maintain its integrity. Typewriters were replaced by word processors but paper was still the final medium for communication. Typically, the integrity of a paper master would be maintained by both parties signing every page.

Today, this can all be done electronically but all the issues of the paper to clay worlds remain. Electronic communications provide greatly improved efficiency and global reach. The question is 'How can electronic mail, and electronic records in general, retain the same properties as those first trade agreements carved out in stone, i.e., integrity, evidence, and non-repudiation?'

1.3 The evolution of email

Most companies now depend on their email systems.

One of the tasks of the IT department is to provide and maintain the corporate email service. Initially this *just* meant choosing a mail system, rolling it out and taking care of day to day administration. (A mail administrator will have a wry smile at the *just*!)

IT has had to solve a number of other issues over time. Lack of interoperability is now a fading memory but spam and the email-borne virus remain major issues. The use of email to communicate pornographic or other unsavoury material has led to the use of content scanning software, as has the requirement to protect corporate information.

The growth in the volume of email has led to IT introducing deletion policies and putting limits on mailbox sizes. IT is now deploying archive systems to help users manage their own mail files and improve the efficiency of the email systems.

These are all fire fighting tactics taken to maintain a service. None of them resolves the problems that clay tablets were first used for – providing integrity, evidence, and non-repudiation.

Ensuring our electronic communications have these qualities is the essence of compliance, and underlies much of the specific industry regulations, as will be explained in this paper.

Due to concerns over these issues, some organisations veto the use of email with customers and partners, so losing a valuable productivity tool, but this still does not eliminate the risks.

1.4 Implications of not being compliant

Every email should be considered as being equivalent to a paper communication. It is because of this that IT alone cannot resolve the issue of compliance. The issue is one of corporate responsibility and good governance for the Board and senior managers of an organisation to address [23]. Whereas virus attacks have visible consequences, compliance, or the lack of it, is often still seen as an irrelevant part of the risk equation of doing business. This situation is starting to change.

The failings of organisations such as Enron and Arthur Anderson have brought the situation to a head. Emails are recognised as a source of evidence for the courts and legal discovery subpoenas are increasingly being issued against organisations. The courts are penalising organisations for failing to produce the requested records, either through contempt of court proceedings, or, by finding against them. It is deemed irrelevant whether the organisations could not deliver the information because of their negligence or because of deliberate or accidental deletion. The levels of fines are increasing. Where organisations continue to ignore or defy the law, the regulators are targeting directors and individual perpetrators. The stakes are getting higher with gaol sentences being seen as the next step.

Back-up and archive systems are not enough as illustrated by a recent case in the US [30]. Uncertainty as to whether or not to retain documents is immaterial. In another recent US case it was held that:

“it is well established that where a party can reasonably anticipate litigation, i.e., it knew or should have known of the potential litigation, it has a duty to preserve evidence that may be relevant to that litigation [28]”

Though in some cases there may be some uncertainty as to the need to keep records, the case also held that:

“it is more reasonable for a party to preserve evidence, in view of the possibility of litigation, than to dispose of it.”

1.5 What needs to be done

Increasingly, regulators are imposing duties on directors and senior managers to ensure that they implement IT solutions that meet their risks and requirements [23].

The organisation must assemble a team which should be approved at board level. Because compliance is corporate wide but impacts at the department level, the team must consider the collective input from individual departments and business units in order to establish the requirements and the solution. The team itself will typically include individuals from IT, HR, legal, internal audit, and other relevant business divisions.

The process must consider all the issues, ascertain the jurisdictions, laws and regulations that apply, work out what needs to be done, prioritise the tasks and create a plan to implement the solution. This will not be an easy journey, but achieving compliance is something only the organisation can do. Rushing out and buying a product without the right preparation is not the right strategy. Appropriate tools will feature in the total solution but they alone cannot make an organisation compliant. It is the organisation, not the product, which must be compliant.

Doing nothing is also not an option; even an organisation with a policy that allows no external business email must take some action. Internal emails are just as important.

1.6 Benefits of Compliance

Meeting the issues of legal and regulatory compliance is not without business benefits -it is not just an insurance policy. A compliant solution will archive all mail messages. This will provide operational benefits for IT and end users. (Note: a compliant solution provides an archive capability; an email archive solution does not necessarily provide compliance.)

On the risk reduction side, an organisation will be able to respond to discovery notices and defend itself with the best evidence if a compliant system is in place. This implies better corporate governance and reduced potential exposure and costs for litigation.

Users are less likely to abuse the mail system and will fully understand the implications of an email message if they know that all messages are automatically archived, whilst organisations will have the evidence to protect themselves against false claims. For instance in a recent case, an organisation managed to protect itself against a claim of sexual harassment as it had archived copies of email messages with sexual overtones sent by the female litigant.

For financial services, a compliant email system will play into the Basel II arena and reduce the capital adequacy ratio.

As more email-related cases come to court and organisations lose partly as a result of a lack of compliance, it should be possible for compliant organisations to negotiate cheaper insurance premiums.

2 THE RULES AND REGULATIONS

2.1 The Law Applies

Anyone who has looked into this area will have read about record keeping regulations, and wrestled with the dichotomy of Data Protection verses the need to monitor mail. These are relevant issues, but underpinning everything is a basic principle – the law. The law applies to electronic documents and communications in exactly the same way that it applies to other forms of documents and communications.

This situation has been clarified by most jurisdictions enacting specific regulations to legitimise electronic communications such that courts cannot deny legal validity on the grounds that a document, record or communication is in electronic form [7], [9], [14], [17], [18], [19], [37].

A problem occurs because the legislation discusses legal impediments to doing business electronically but not the practical issues [10]. One result of this is a pre-occupation on topics such as Electronic Signatures and record keeping requirements. Both are important, but must be seen in the basic legal context of evidential weight.

Evidential weight requirements do not apply to bundles of records. They apply to each record individually.

2.2 Evidential Weight

The legislation referred to above provides for legal admissibility of evidence in a Court of Law. It is for the court to decide how much it will trust the information – what evidential weight to attach to the evidence. Evidential weight is about reducing the uncertainty surrounding evidence [5], [16]. The side with the greater evidential weight will usually win, or at least mitigate its liability.

Compliance should be considered as providing evidential weight for electronic data that can match the evidential weight of paper. This is much more than records storage. It concerns the whole lifecycle of data creation, transmission, storage and eventual controlled deletion. The challenge is to overcome the inherent transient nature of electronic data and requires that all aspects of data are retained; the existence or occurrence of the data, the data itself, any access to the data contents, any attempt to edit or delete the data, ensuring that the data created is the data that is stored and demonstrating that no data has been lost or inappropriately deleted.

At heart here is the principal captured in every jurisdiction, which is to affirm the weight of the evidence.

2.3 Data protection

Data protection is all pervasive in the European Union [12]. If organisations process personal data then they must ensure that they comply with the limitations placed on them by the Directive and respective implementation laws in the Member States of the EU [6].

Organisations must ensure that any data is processed fairly and lawfully, kept secure from unauthorised access, and deleted once it is no longer required. Within the EU organisations must satisfy data subject requests and within a set time.

A common misconception is that there is a dichotomy between the need to keep records and data protection requirements. No such dichotomy exists. An organisation has the right and duty to retain data in order to protect itself in case of legal action. This can include personal or private emails. These, however, must not be read by the organisation unless needed for a legal action. The organisation must simply ensure that records can only be used for prescribed purposes, and that it deletes any records that contain personal data once the required retention period has come to an end [11].

2.4 Data privacy and monitoring

Workers are entitled to a degree of privacy in the work place [20] which organisations have a duty to respect, and includes the ability to send personal and private emails. Organisations can still establish evidential weight for their electronic communications, but they must understand the difference between establishing evidential weight and monitoring [20], [35]. Organisations may not, except in certain circumstances, read private messages, but they can scan such messages for viruses or spam, or in some cases monitor traffic patterns. Establishing evidential weight requires that records are kept for the required retention period or until they are no longer needed. The records should not be opened or read unless or until they must be, and employees must be kept fully aware of this activity and their organisations' policies.

In some jurisdictions users must be able to delete their private records irrespective of any retention policy.

2.5 Record Keeping Requirements

There is a general requirement to maintain adequate records as a requirement of doing business, though some industries, especially those that are regulated, have additional onerous requirements.

2.5.1 General commercial requirements

Record retention requirements for electronic data are the same as those for paper records. Minimum time limits are defined for various record types, such as companies' documents and records, contractual documents and communications, negotiations, employment records, tax records, general commercial communications, though in virtually all jurisdictions there is also a general duty to keep documents until there is no longer the possibility of their use in litigation.

If an organisation does business in different jurisdictions then foreign regulations will also apply. The most notable example of this is the Sarbanes-Oxley Act of 2002 (US), of which section 409, a requirement for real-time reporting systems, is particularly onerous [31].

2.5.2 Financial services

Financial service providers have stringent record keeping, monitoring, and supervision requirements. Every jurisdiction defines the records that it wants kept together with their retention periods. Retention periods are set on a per record basis. Simply relying on the provisions of general company law is insufficient. The regulations under the Financial Services and Markets Act [21] and the Financial Services Act in the UK define a huge array of retention

requirements, most of which are summarised in the Financial Services Authority Handbook. The requirements for both retention and deletion must be met.

If the providers are subject to the SEC then they need to meet the requirements under rules 17a-3 [32] and 17a-4 [33] of the Securities and Exchange Act 1934 which set out in great detail the standards and safeguards that archival systems must provide. These requirements do not discriminate against electronic storage; they simply bring the standards up to those of paper-based systems.

Basel II is a growing issue globally and requires extensive reporting systems in order to facilitate the risk management models that will allow financial services to reduce their respective capital adequacy ratios. Whilst officially applicable to banks, financial service regulators around the world seem set on implementing and extending the regime to cover all forms of financial service providers. A system that ensures evidential weight will form the basis of the reporting requirements for Basel II [2].

2.5.3 Pharmaceuticals and Health Care

In the US the Food and Drug Administration has developed a set of regulations, 21 CFR Part 11 [1], that mandates the procedures that pharmaceutical and bioscience companies must follow with regards to electronic records, and electronic signatures. These procedures are intended to establish the validity and integrity of the records where organisations wish to use electronic information and communication systems.

Patient record confidentiality is a major concern. The Data Protection Directive in Europe applies and codes are being produced by the Member states to ensure compliance in this area. In the US the Health Insurance Portability & Accountability Act 1996 mandates requirements for patient record privacy and protection with regards to electronic records and transactions [25].

2.5.4 Telecommunications

Many jurisdictions require telecommunications service providers to retain communications data for a period of time in the event that it may be required for future criminal investigation. Within the EU codes and regulations must be drawn up to comply with the Data Protection Directive. In the UK a voluntary code of practice stipulating the retention periods, from 3 to 12 months depending on the type of record, has been drawn up under the Anti Terrorism, Crime and Security Act 2001. Other Member States have enacted similar provisions.

In the EU, the Directive on privacy and electronic communications requires stringent record management and deletion procedures. Personal data must be stored securely, but only so long as it is required after which it must be deleted. Recital 23 makes this clear [11].

2.6 Other Issues

2.6.1 Pornography and paedophilia

Paedophilia is strictly prohibited. Mere possession, even unknowingly, is often enough to secure a conviction and custodial sentence (in some jurisdictions, such as in Denmark, although freedom of expression is protected and paedophilia can be discussed, the possession of paedophilic material is still prohibited). If paedophilic material is detected it should not be

deleted or processed. Rather the authorities should be contacted immediately and any action taken in conjunction with them. Pornography is generally thought of as less serious, but it is regulated differently by different jurisdictions. What is acceptable in one jurisdiction may incur criminal liability in another. Legal advice should be sought.

2.6.2 Spam, anti-virus, content checking

ISPs may be required to begin filtering Spam. Originators of spam and viruses may be held liable for any damage caused. For instance in Italy an organisation can be held liable if a virus is sent from its own internal network.

2.6.3 Electronic/digital signatures

Regulators in most jurisdictions have recognised the validity of electronic signatures [8], [13], [15], [34], [36], and provided for their legal validity. None of the implementing legislation guarantees evidential weight for electronic signatures. They simply prevent the courts from denying admissibility due to their electronic form. The evidential weight of the signatures must still be ascertained. Though virtually any form of signature may be used, in practice only a properly implemented digital signature will attract any real evidential weight in a dispute.

2.6.4 The Postal Rule

The postal rule has caused some confusion with regards to its application to electronic mail.

The postal rule is a peculiarity of English law although similar rules exist mainly in common law jurisdictions; a few civil law jurisdictions also have rules that have a similar effect. The postal rule is an exception to the general rule of contract formation which is that an acceptance is only effective when it is received by the party making the original offer to contract. The postal rule applies only when the parties to an agreement do not communicate with each other by way of instantaneous communications such as by telephone but instead use a non-instantaneous method of communications such as the postal service. Put simply, the rule states that an acceptance is effective once it is posted, rather than when it is actually received. The essence is that the acceptor has entrusted his communication to a trustworthy third party.

This may seem to be relevant to electronic mail, which is a non-instantaneous method of communication. However this is not the case, because the postal rule only applies where the parties trust their communications to a third party which can be trusted to deliver the communications. Electronic mail cannot be relied upon to deliver a communication.

The postal rule is not a hard and fast rule but is simply a presumption that is easily rebutted. If the terms of the offer to contract state that the acceptance must be received by a certain time or date then the rule does not apply.

3 REQUIREMENTS OF THE SOLUTION

The list of rules and regulations can seem daunting but fortunately, the requirements can be broken down into seven core areas: record capture, record storage, record retrieval, access controls and authentication, record integrity, proof of delivery, audit, and disposal which together provide non-repudiation and evidential weight. The BSI tackled this issue in 1999 and created an international code of practice, updated in 2002, BSI DISC PD5000:2002. This code contains five parts of which BSI DISC PD0008:1999 (shortly to be adopted internationally as ISO TC15801), is a mandatory component and concentrates purely on the storage of electronic information. However, it should be noted that the BSI code of practice is merely a starting point, and not the ultimate description of what is required in order to achieve full evidential weight.

3.1 Core requirements

The core requirements are based on the need to provide non-repudiation and evidential weight.

3.1.1 Record capture

A storage system is irrelevant if a system cannot guarantee to capture the information correctly and retain its integrity from that point on. A message coming into the organisation must be captured along with all its context, uniquely identified and its integrity guaranteed, and then archived before it is processed in any other way. This demonstrates that it is impossible to alter or delete the message before storage. Relying on a mail system's journaling functionality is not foolproof and allowing end users to define what is archived and when is totally unacceptable.

If record creation is not routine or timely, then it may not survive a "hearsay objection" from opposing counsel.

A message leaving an organisation must be archived after all other processing has taken place. Legally, liability rests with the organisation rather than an individual, so it is important to capture the message sent by the organisation. A compliant system may well want to ensure that the final message sent is the original message sent by the sender.

Note, the sender only has to demonstrate that a message reaches the recipient organisation in a form readable by that organisation. It is then that organisation's responsibility to process the message correctly.

3.1.2 Record storage

Each record, along with any supporting information, must be stored for its mandated retention period which should be identified and documented. A default retention period for each record will be the minimum period of all record types. Automated analysis or human intervention may extend this period, so a solution must support retention time extension at the individual record level.

Storage subsystems may exhibit the ability to maintain data integrity but a fully compliant *system* must demonstrate record integrity from the time a message reaches or leaves the organisation until deletion. This is partly covered by capturing the record when it first reaches the organisation but also includes technologies such as digital signatures.

3.1.3 Record retrieval

A solution that stores data but does not allow retrieval is worthless [30]! Record retrieval must, however, be restricted to those who have authorisation to retrieve the relevant messages. A user obviously must be able to retrieve messages that he has sent or received. The organisation and regulations will define further controls. For example, a privileged user must be able to carry out a discovery operation across the whole archive but restrict the visible messages to those that are relevant. To do so will require a powerful searching mechanism. Under certain circumstances, a privileged user may be able to look at another person's records. Such accesses must be controlled and must be audited. Unauthorised attempts to access records must be denied, but must also be audited.

In the USA, a response to an SEC discovery notice for certain records is required in 36 hours; in the UK a similar notice from the FSA requires a response in 24 hours [22]. The archive must be capable of responding well within these time frames, requiring online and/or near term backing storage. This may also provides operational benefits such as recovering an end user's mailbox and reduces the requirements on server backups and restores.

3.1.4 Access Controls and Authentication

A user may only carry out the operations on the archived records for which he is authorised. An end user, or privileged user, must first authenticate to the record storage system in order to retrieve permitted records and can only carry out the operations that the role permits.

There must be strong access controls in place to prevent the accidental or malicious deletion or alteration of records. The access controls must be enhanced by strong authentication and permission management controls to allow the deletion or alteration of records due to the expiry of their retention periods, or alteration is required due to a court order or some other operation of law.

3.1.5 Record integrity

Preserving and proving record integrity is vital. A compliant solution will need to utilise cryptographic tools and digital signature technologies internally to audit and guarantee that the stored record is identical to the captured record during its retention lifetime.

The integrity of each record should be established and audited from the moment of its creation and will need to be verified:

- At the moment of capture by the system at the moment of transmission and receipt;
- During the lifetime to prevent loss or damage due to bit-degradation;
- On retrieval; and
- On controlled deletion to verify that the selected record is being deleted.

Risk can be further reduced by the sender first establishing integrity and the recipient verifying it.

3.1.6 Proof of delivery and non-repudiation

Proof of delivery means more than just proving that the message was received. It includes the proof of who sent the message, it includes the proof that the message integrity has been preserved, and it includes the proof that the message was received in a format that the recipient could read if they so chose to do. Proof of delivery itself is part of non-repudiation. True non-repudiation is not just simply proving the sender sent a message; in its entirety, non-repudiation means:

- The sender can prove that he sent the message;
- The sender can prove that the recipient received the message in a form that the recipient could read;
- The sender can prove that the message sent was the message delivered and in the form that it was sent;
- The sender can prove that the message has not been altered in any way;
- The sender can prove that his copy of the message has not been altered in any way;
- The sender can prove that the copy of the message that was sent was archived at the point of transmission before any alteration was possible;
- The sender has a full audit trail of the message;
- The recipient can prove that the sender sent the message;
- The recipient can prove that he received the message;
- The recipient can prove that the message received was the message sent and in the form that it was sent;
- The recipient can prove that the message has not been altered in any way;
- The recipient can prove that his copy of the message has not been altered in any way;
- The recipient can prove that the copy of the message that was received was archived at the point of reception before any alteration was possible; and

Authentication has a part of play in this process:

- In keeping with the role of the organisation as a legal entity, email systems should authenticate to each other to demonstrate that a message has been sent to the right organisation; and
- To remove the possibility of mail spoofing, end users should have the ability to mutually authenticate, though this is not a legal requirement itself as liability rests with the organisation.

3.1.7 Audit

Audit is the functionality most often overlooked. It is vital that a separately stored record audit is maintained. An audit needs to record all accesses, attempted access, changes and any other activity on *each and every record*.

The separation of audit information from the record ensures that it can be proved that a record hasn't been deleted before its expiry date or that any operation done on the record is legal. An example of where audit is fundamental is deleting a record before its expiry date as a result of a court order. The deletion and reason for deletion must be fully audited although the record will no longer exist.

Audit information on a record should be kept for a period after record deletion in case the integrity and veracity of the record store and audit trail is questioned at a later date.

3.1.8 Record Disposal

It must be possible to delete (expunge) or alter a message if required to do so by law, and it is this requirement that makes optical media an unacceptable email archive medium. This requirement can seem to be at odds with SEC 17a but note the potential for personal data as well as company records. There are two scenarios: expired personal messages and legal intervention.

- Once the retention period has expired, any records containing personal data must be deleted. As it is an employee's right to use email for private mail (with limitations defined in the Use Policy) this is a real issue for an email archive. It is an organisation's choice whether to delete an expired record which does not contain private data. Once a record's strict legal retention period has come to an end it may be time barred from any subsequent action.
- There may be a legal demand, by operation of law or by court order, to change or delete a record before the expiry of the retention period. This places stringent requirements on access controls and authorisation rights on the email archive solution and, along with all other operations, must be fully audited.

Components that do not allow for controlled deletion cannot be used to create a system that complies with the data protection laws within the EU.

3.2 Other requirements

3.2.1 Confidentiality and secure email

The regulations of data protection and good corporate governance require confidentiality of personal data and corporate information. Encryption should be used when sending information across the Internet and ideally within the organisation as well.

A record store may also use encryption to ensure the confidentiality of the information stored within. Strong access controls to the archive are essential with a full audit of all access attempts.

If an organisation uses encryption then it may be subject to the provisions regarding access to information protected by encryption in the Regulation of Investigatory Powers Act 2000 [29].

3.2.2 Supervisory requirements

Various regulatory bodies, such as the FSA [24] in the UK and the National Association of Securities Dealers [26], [27] in the US, impose a requirement for senior management to be able to supervise communications in their organisations to ensure that regulations are complied with. The access controls of the record storage system should allow authorised personnel controlled

access to relevant records in order to facilitate the supervision requirements, and should be flexible enough to allow full supervision to take place. Such access should be fully audited.

3.3 Requirements of a useable mail system

A solution that meets the legal and regulatory requirements has to be usable and manageable. There are a number of additional requirements that should be considered part of the total solution which either the compliant solution must integrate with or the compliant solution should enable the extra capability.

The solution must integrate with anti-virus, spam filtering and content analysis utilities. These must operate before a message is archived where it is being sent, and after it has been archived if it is being received. In those jurisdictions where it is legal to use utilities that add disclaimers to a message before it is sent, this must be done before the archive process. For a full audit trail, the message as sent by the user before processing by content checking, anti-virus, or disclaimer addition, should also be archived.

Operationally, the solution must reduce the backup burden on the mail server and provide user recovery. From an end user viewpoint, the existence of the solution should be transparent but at the same time provide access to the knowledge store.

4 PUTTING COMPLIANCE INTO PRACTICE

If an organisation is to begin to achieve compliance then it must assemble a team which should be given a mandate by the board. Input from every department and business unit will need to be considered in order to establish the requirements and the solution.

4.1 Selecting the team

The exact details of any solution will be specific to a particular organisation but there are a defined set of requirements to be met and a common approach that can be taken. It is important not to rush into a quick fix as the correct solution will impact everyone in the organisation. Getting it wrong is little better than doing nothing.

A diverse team will be required to define and approve the solution.

The organisation must decide who will be the leader of this team but one recommendation is that a board-level sponsor is obtained. Failure to comply with regulations or the law has a direct bearing on the liability of directors. The board must ensure that it is kept fully aware of the issues and kept informed of any new risks that may be uncovered.

4.1.1 Legal

Legal will need to ensure that the solution meets all the legal requirements.

4.1.2 Human Resources

Procedures will need to be put in place that will affect all staff. HR will need to be involved in the drafting and distribution of these procedures.

4.1.3 IT Department

The IT department will be central to the implementation of the final solution. IT may have their own requirements that should be met, but IT can only implement a solution once the full set of requirements has been specified by the organisation.

4.1.4 Security

Any impact to IT needs to be reviewed by security. The solution has very real security implications regarding data access and is likely to include a review of secure email.

4.1.5 Risk/Compliance Officer

The Compliance Officer should understand and be able to ascertain the risks faced by the organisation, and be involved in defining the policies, procedures, and systems that the organisation must implement.

4.1.6 The Departments

Compliance involves every department within an organisation, though the individual business units and departments themselves may not form a part of the core team. However they will

provide the information that the team collects. It is essentially the team's task to interview the departments to understand the types of records in use.

4.2 Defining the solution

Two codes of practice are helpful starting points. These are BSI-DISC PD 0008:1999, the Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically [3], and BSI-DISC PD 5000:2002, A Code of Practice in 5 Parts for – Electronic Documents and E-Commerce Transactions as Legally Admissible Evidence [4]. These codes look at the general issues surrounding evidential weight but do not refer to specific industry regulations.

Every organisation will have its own requirements that must be met, but a general outline of some of the points to consider is set out below:

- **Legal & the Board.** What jurisdictions does the business trade under? What regulations apply? This will define the set of laws that need to be adhered to and highlight any clashes and the requirement to implement email policies that depend on the country the sender and/or receiver are located in or doing business in.
- **Legal.** Define a comprehensive document retention policy based on the applicable regulations. A review that begins with email will naturally, and rightly, expand to cover all electronic records created by the organisation and how they are managed.
- **HR & Legal.** Define an email Acceptable Use Policy including disciplinary procedures. Define an education programme for document retention and email use, and implement and monitor it.
- **HR & Legal & IT.** Review the Security Policy. An organisation should have a central Security Policy, some of which impinges on email and record retention. However, compliance is a separate issue from security and is not covered by ISO 17799 or BSI 7799.
- **IT & Security.** IT must consider the operational requirements for any system. The issues of mail server management, backups, archive management, disaster recovery, sizing, throughput etc need to be defined and documented. In fact, this area can easily define a positive return on investment for the final solution.
- **Team.** Build a list of requirements that a solution must/should meet. This list may include groups of functions to allow for a staged implementation.

The project will extend to cover all forms of electronic records and their requirements, and as such will need to be planned carefully with this in mind. All the requirements should be understood before a solution is scoped.

4.3 Components of the solution

The solution must be capable of meeting all of the existing requirements. The solution may be modular in nature, comprising email systems, document management systems, hardware subsystems, procedures, and so forth, but the record storage system will be fundamental to any overall solution.

Fault tolerance and throughput are vital considerations as are longevity and technology renewal.

Magnetic disks should be used to achieve the requirements of fast access for discovery and meet the requirement in the EU to be able to delete or amend individual records. The solution must ensure that records cannot be changed or accessed through a back door as it is a disk [3], [33].

The solution may use various levels of storage, from SANs through to near-line storage for performance and cost reasons. The solution must therefore ensure that it can perform a fully audited, verified, and secure data migration between these levels [3].

Hardware on its own is insufficient, irrespective of its functionality. Specialist software that has been designed specifically to address the requirements discussed in section 3 will be required. Hardware that may be 'compliant' coupled with software that is not compliant cannot be part of a compliant solution. A solution is only as good as its weakest link.

Products alone do not make an organisation compliant. Compliance is only achieved through a combination of hardware, software and procedures, which have been implemented correctly and which are continuously audited and reviewed.

5 CONCLUSION

To implement an email system that provides the strongest evidential weight and meets the legal and regulatory requirements is a difficult but achievable task. It will take time and an organisation should not attempt a solution without first understanding the full set of requirements that the organisation must meet. As with any major undertaking, the organisation must ascertain the requirements and their implications, make a plan based on its business needs and priorities, and then execute that plan.

Some of the requirements may be seen as insurance whilst others have a direct ROI. Whatever the final outcome, doing nothing is not an option. From a legal perspective:

- If an organisation uses a system that it knows is non-compliant then it can be held liable (even though it may be "best of breed").
- If an organisation knows of a system that is compliant but fails to use it then it can be held liable.

The bottom line from a legal perspective – if an organisation cannot use a compliant system then it should not communicate via electronic mail!

6 REFERENCES

- [1] 21 CFR Part 11. Defined by the Food and Drug Administration (US) to mandate the procedures that pharmaceutical and bioscience companies must follow with regards to electronic records, and electronic signatures. www.21cfrpart11.com
- [2] Basel Capital Accord, Basel II , Bank for International Settlements, Jan 2001. All banks will have to meet the requirements by 2007 but should meet by 2004 to achieve 3 years of records. Likely to extend to all financial institutions. www.bis.org/publ/bcbsca.htm.
- [3] BSI-DISC PD 0008:1999, The BSI Code of Practice for legal admissibility and evidential weight of information stored electronically. Defines what practically needs to be done and also covers the issues of scanned documents. www.bsi-global.com/Portfolio+of+Products+and+Services/Books+Guides/Doc+M+anagement/pd0008.xalter
- [4] BSI-DISC PD 5000: 2002, The BSI Code of Practice for Legal Admissibility of Electronic Documents and e-Commerce Transactions. A 5 part code, of which PD 0008 is part 1, covering storage, communications, identification and signatures, using certification authorities and using third party archives. www.bsi-global.com/Portfolio+of+Products+and+Services/Books+Guides/Doc+M+anagement/pd5000.xalter
- [5] Civil Evidence Act 1995, section 4(1). Changed the focus on evidence and looks to the weight of the evidence rather than its admissibility. This mirrored changes in other Common Law jurisdictions and the approach in Civil jurisdictions. www.hmso.gov.uk/acts/acts1995/Ukpga_19950038_en_1.htm
- [6] Data Protection Act 1998. One provision allows a court to order retrieval of specific personal data. www.hmso.gov.uk/acts/acts1998/19980029.htm
- [7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Article 5. Removed all doubt as to whether or not parties can use electronic documents and messages for commercial transactions and communications. europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf
- [8] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf
- [9] Directive 2000/31/EC of the European Parliament and of the Council of 08 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, article 9. Removed all doubt as to whether or not parties can use electronic documents and messages for commercial transactions and communications. europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf
- [10] Directive 2000/31/EC of the European Parliament and of the Council of 08 June

2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, recital 37.
europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

- [11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Personal data must be stored securely, but only so long as it is required after which it must be deleted. Recital 23. (Telecoms)
europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf
- [12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , article 3, Data Protection Directive.
europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett
- [13] Electronic Communications Act 2000. Removed all doubt as to whether or not parties can use electronic documents and messages for commercial transactions and communications. www.hmso.gov.uk/acts/acts2000/20000007.htm
- [14] Electronic Communications and Transactions Act 2002 (South Africa), article 15. www.gov.za/gazette/acts/2002/a25-02.pdf
- [15] Electronic Communications and Transactions Act 2002 (South Africa). www.gov.za/gazette/acts/2002/a25-02.pdf
- [16] Electronic Communications and Transactions Act 2002 (South Africa), ss 15(2), 15(3). www.gov.za/gazette/acts/2002/a25-02.pdf
- [17] Electronic Signatures in Global and National Commerce Act 2000 (US), s101. [www.fca.gov/apps/infomemo.nsf/59ab19ff3b724b73852569530076c529/4706c31b43af553985256c080042e071/\\$FILE/E-Signatures.pdf](http://www.fca.gov/apps/infomemo.nsf/59ab19ff3b724b73852569530076c529/4706c31b43af553985256c080042e071/$FILE/E-Signatures.pdf)
- [18] Electronic Transactions Act 1999 (Australia), article 8. www.nationalsecurity.gov.au/agd/Department/Publications/publications/ecommerce/ElectronicTrans_Act.html
- [19] Electronic Transactions Ordinance (Hong Kong), article 5. www.info.gov.hk/digital21/eng/ecommerce/etb/etb.html
- [20] Employment Practices Data Protection code of practice, Part 3, from the UK Information Commissioner. www.dataprotection.gov.uk/employcop.htm
- [21] Financial Services and Markets Act 2000. Defines a huge array of retention requirements, most of which are summarised in the Conduct of Business Source Book. There is no distinction between paper and electronic form. The requirements for retention and deletion must be met. www.hmso.gov.uk/acts/acts2000/20000008.htm
- [22] FSA Handbook, Interim Prudential sourcebook: Investment business, Rule 5.3.1(6). Requires information to be delivered up within 24 hours. www.fsa.gov.uk/handbook/

- [23] FSA Handbook, Interim Prudential sourcebook: Investment business, Rule 3.13(5). "A firm must maintain adequate procedures for the maintenance, security, privacy and preservation of records, working papers and documents of title belonging to the firm or others so that they are reasonably safeguarded against loss, unauthorised access, alteration or destruction."
www.fsa.gov.uk/handbook/
- [24] FSA Handbook. www.fsa.gov.uk/handbook/
- [25] Health Insurance Portability & Accountability Act 1996.
www.cms.hhs.gov/hipaa/.
- [26] NASD Rule 2210.
cchwallstreet.com/nasd/nasdviewer.asp?SelectedNode=3&FileName=/nasd/nasd_rules/RulesoftheAssociation_mg.xml#chp_1_3
- [27] NASD Rule 3010,
cchwallstreet.com/nasd/nasdviewer.asp?SelectedNode=3&FileName=/nasd/nasd_rules/RulesoftheAssociation_mg.xml#chp_1_3
- [28] RAMBUS, INC, the adjudication proceedings before the FTC in the Matter of RAMBUS, INC, 2002, Docket No 9302. www.ftc.gov/os/adjpro/d9302/
- [29] Regulation of Investigatory Powers Act 2000.
www.hmso.gov.uk/acts/acts2000/20000023.htm
- [30] Residential Funding Corporation v DeGeorge Financial Corp., DeGeorge Home Alliance, Inc. and DeGeorge Capital Corp, Docket No 01-9282. In a recent case, the US Court of Appeals for the Second Circuit held that a party could be held liable for failure to deliver electronic evidence even if the unavailability was not caused by gross negligence or bad faith of that party.
laws.lp.findlaw.com/getcase/2nd/case/019282&exact=1
- [31] Sarbanes-Oxley Act of 2002 (US), of which section 409.
www.sarbanes-oxley.com/pcaob.php?level=1&pub_id=Sarbanes-Oxley
- [32] SEC Rule 17a-3 under the Securities and Exchange Act 1934.
cchwallstreet.com/nasd/nasdviewer.asp?SelectedNode=7&FileName=/nasd/sec_rules/secrules_mg.xml#chp_1_7_2
- [33] SEC Rule 17a-4 under the Securities and Exchange Act 1934.
cchwallstreet.com/nasd/nasdviewer.asp?SelectedNode=7&FileName=/nasd/sec_rules/secrules_mg.xml#chp_1_7_2
- [34] Signatures in Global and National Commerce Act 2000 (US).
[www.fca.gov/apps/infomemo.nsf/59ab19ff3b724b73852569530076c529/4706c31b43af553985256c080042e071/\\$FILE/E-Signatures.pdf](http://www.fca.gov/apps/infomemo.nsf/59ab19ff3b724b73852569530076c529/4706c31b43af553985256c080042e071/$FILE/E-Signatures.pdf)
- [35] Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, SI 2000/2699.
www.legislation.hmso.gov.uk/si/si2000/20002699.htm

- [36] Uniform Electronic Transactions Act (US).
www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm
- [37] Uniform Electronic Transactions Act 1999 (United States), section 7.
www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

7 FURTHER READING

1. National Archives and Records Administration, NARA GRS20 (US Federal Government). ardor.nara.gov/grs/grs20.html
2. US DOD 5015.2. www.dtic.mil/whs/directives/corres/html/50152std.htm
3. Fortune European Edition, Volume 146, No 12 December 30th, 2002. UBS Warburg were quoted as claiming that the cost of producing subpoenaed electronic mails was in an eight-figure range and would take up to approximately two years to achieve. The SEC requires the information within 36 hours.
4. Fortune European Edition, Volume 147, No 5, March 17th 2003. Aside from regulatory requirements the law in general requires that users, especially commercial users, retain their records until any potential legal action has ceased to exist. Litigators have discovered that email records, or rather the lack of such records are an ideal tool to use to win cases.
5. BS 7799 (ISO/IEC 17799) is the accepted International Standard for Information Security Management. www.bsi-global.com/Corporate/17799.xalter
6. Fortune European Edition, Volume 147, No 3, February 17th 2003. Electronic mail has become a prime source of evidence

	Financial Services	Governments	Pharmaceuticals	Defence / aerospace	Healthcare	Professional Services	Telecommunications
USA PATRIOT	US	US	US	US	US	US	US
Electronic Signatures in Global and National Commerce Act	✓	✓	✓	✓	✓	✓	✓
Healthcare Insurance Portability and Accounting Act (HIPAA)			✓		✓		
Financial Services Modernization Acts	US						
Securities and Exchange Act 1934 rule 17-a4	✓					✓	
European Directive on electronic commerce	EU	EU	EU	EU	EU	EU	EU
European Directive on distance selling	EU		EU			EU	EU
European Directive on distance marketing of financial services	EU					EU	
European Directive on electronic signatures	✓	✓	✓	✓	✓	✓	✓
European Directive on electronic invoicing of VAT	✓	✓	✓	✓	✓	✓	✓
European Directive on privacy and electronic communications	EU	EU	EU	EU	EU	EU	EU
UK Civil Evidence Act	UK	UK	UK	UK	UK	UK	UK
UK Police and Criminal Evidence Act	UK	UK	UK	UK	UK	UK	UK
UK Regulation of Investigatory Powers Act	UK	UK	UK	UK	UK	UK	UK
UK Financial Services and Markets Act	✓					✓	

ABOUT THE AUTHORS

Lars Davies is a Senior Visiting Fellow to the Institute for Computer and Communications Law, Centre for Commercial Law Studies at Queen Mary, University of London. He specialises in Information Technology Law, Internet Law and Telecommunications Law and currently concentrates on issues that include electronic financial services, security, authentication, and regulatory compliance.

He joined the Institute in 1995 as a full-time academic. During his time as an academic Lars consulted to a city firm of solicitors on a range of legal and regulatory issues relating to telecommunications and electronic commerce. Prior to becoming a lawyer, Lars worked in the computer industry.

Lars is a frequent and well known speaker on these topics and is widely published, including contributions to the telecommunications volume of the Encyclopaedia of Forms and Precedents.

Lars left his post in 2002 and is now the CEO of Kalypton Limited, a company he formed to deliver solutions that enable users to achieve regulatory compliance and evidential weight for their electronic communications. He continues to consult to a variety of concerns.

Ian Walker has worked in the IT industry for nearly 30 years of which the last 8 have concentrated on internet security and solutions utilising public key infrastructures. Ian has been a regular speaker on the subject and contributed to numerous articles.

Prior to his current position, Ian spent 5 years as technical director of Entrust (Europe) Ltd, a leading supplier of PKI, digital identity and internet security solutions.

Before joining Entrust, Ian spent nearly 20 years at EDS (formally SD-Scicon) working in all aspects of product development, management and sales, creating advanced software development products for the defence and aerospace industries.

Ian is currently the chief operating officer of Kalypton Ltd a company formed to deliver solutions that enable users to achieve regulatory compliance and evidential weight for their electronic communications.