



Total Control of Your
Corporate Intelligence

**EMAIL:
A Best Practice
Approach to
Compliance
& Information
Management**

A ZANTAZ White Paper compiled
by Alan Calder, IT Governance Ltd

Contents

Executive summary	3
Introduction	4
Operational management issues	5
Regulatory requirements	6
Litigation risk	9
Best-practice guidance	10
ISO/IEC 17799:2005	11
ISO 15489, the BSI Code of Practice and MoReq	12
Conclusion	13

Executive summary

Email is fundamental to organizational communication. Significant costs and risks are associated with the business use of email, including operational, regulatory, and litigation risk. These risks are changing and evolving and organizations should use a best-practice framework to guide their response to them. An end-to-end email management, retention, maintenance and archiving solution will enable organizations to meet current and emerging business and regulatory requirements.

Introduction

Email is today the key means of internal and external communication for many organizations. In the UK, the DTI Information Security Breaches Survey 2004 confirmed that **87% of UK businesses saw themselves as “highly dependent” on electronic information.**

Email is often informal and frequently cryptic, but it underpins external contract negotiations, with both customers and suppliers, and supports the entire transaction cycle from initial enquiry through to post-sales support. Requirements, specifications and deliverables are explored, defined, priced and agreed using email. Complaints, queries and their resolutions are managed through the corporate email box.

Email is intrinsic to corporate communication

“The importance of email in underpinning the entire range of organizational communication, and the business risks associated with its use, have made email management a critical IT and board governance responsibility.”

Internally, email usage is intrinsic to corporate communication, project progress and human resource management.

Guidance, mentoring, support and individual views and responses are all canvassed or dispensed electronically. Most decisions about promotion, demotion, hiring, firing, rewarding or disciplining staff involve a significant amount of

email communication between a number of people, some of whom, such as lawyers and recruitment consultants, may not even be within the organization.

Business risk and email

Email can be used to commit the organization to expenditure or a course of action that has not been approved, or whose risks have not been fully assessed. It can also be used nefariously. Crucial, sensitive or confidential information can be cut and pasted into an email and sent to an external party both easily and quickly. Commercially important documents, including price sensitive information and intellectual property, can be attached to an email and sent half-way round the world to a competitor, or a potential attacker, in an instant.

Email can also be used in breach of legislation such as the Human Rights Act to harass, intimidate or otherwise demean bosses, co-workers and more junior staff. It can be used for sexual, racial and other abuse.

Governance and risk management

The management of risk is a fundamental part of today's corporate governance environment. Boards of directors are expected to identify critical business risks and ensure that adequate and appropriate steps have been taken to minimize them. The dependence on email and electronic information means that email management has become a critical responsibility for IT management, and a key element of the Board's overall responsibility for IT governance.

Email has also become a major concern for regulatory authorities at the same time as it has become of significant interest to lawyers, and specifically to litigators.

IT managers and boards should view their email management responsibilities under three headings:

- Operational issues,
- Regulatory requirements, and
- Litigation needs.

Email management solutions should deliver end-to-end solutions against requirements identified under each of these headings.

Operational management issues

The two biggest operational email management challenges are both caused by:

- The inexorable growth in global email volume (a compound annual growth rate of 44%¹ reaching 3,390 Petabytes² of data by 2006) and,
- The decentralization of business communication and record keeping that email has made possible

In the paper age, secretaries typed letters. Early drafts of documents were usually destroyed when the final, approved document was signed off and issued, whether to an internal or external recipient. Copies of correspondence were stored in serried ranks of filing cabinets, and older documents were archived off site.

In the email age, communication is rarely filtered through a secretarial control process; emails are written and despatched, usually without revision, let alone formal review. In effect, every business email user can use the corporate email system to issue a communication that represents – and which may bind – the company. **Every one of these communications, however brief, is a corporate record.**

Increasing data storage requirement

The proliferation of email, with its instant 'copy to' feature, has made email inbox capacity management and secure email archive storage increasingly important as organizations recognize the level of hardware investment required to sustain this growth in their electronic data storage needs.

Many organizations try and manage their email volume challenges by imposing email box sizes on users. These solutions, configured at the corporate level on the email server(s), typically warn users that they are approaching a pre-set size limit for their email boxes and, once they have reached the limit, stop the user either sending or receiving further emails.

The disadvantages of user restrictions

This approach is usually effective in controlling the data storage requirements on the email server, as it forces users to delete emails and email attachments they think they won't need, or to archive their emails, usually using the email application's archive facility.

As an operational solution, this approach has at least four disadvantages:

- It can mean that recipients sometimes never receive the email they've been sent;
- From time to time, the need to selectively delete emails stops users from getting on with their jobs;
- It allows users to delete emails that might, at some later date, be of crucial importance either to them or to the organization in dealing with a legal, contractual or other key business issue; and
- It creates email archive files, usually on workstation hard drives, that are not backed up centrally, which therefore fall outside the corporate business continuity and disaster recovery policies, and may at some future point be unavailable to the organization.

From a regulatory viewpoint, these operational disadvantages become severe weaknesses.

¹ IDC 2004, Network World (2003) Socha/Gelbman (2004)

² 1 Petabyte = 1 Million Gbs = 1 Billion Mbs

Regulatory requirements

Regulatory requirements in respect of information and email are complex, still emerging and fast changing. They overlap and contradict one another, and have not yet been properly tested in the law courts. While the method of compliance is still not clear, the penalties for failure are. These regulations can be defined as follows:

Data retention requirements

- Data protection (and freedom of information) requirements
- Internal control requirements
- Audit trail and compliance requirements
- Retention requirements

Every country in the world has corporate legislation that specifies the length of time for which organizations must retain their corporate records. Most of this legislation pre-dates the Internet and email, and doesn't differentiate between paper-based communications and records, and electronic ones. The requirement is simply that the organization retains all its records for a specified period of time.

By default, this record retention requirement includes email.

Specified retention periods for company records are not necessarily in line with the time period during which the tax authorities can initiate an investigation into the company's affairs, or even the national Statute of Limitations in respect of criminal or health and safety law. In addition, sectoral regulators (financial or medical regulators, for instance) may impose other retention periods. These differing retention requirements apply to email in just the same way as they apply to other documents.

From a governance perspective, boards need to ensure they preserve their corporate information for appropriate time periods, determined by reference to the type of information and the relevant legislation. Organizations usually do this by creating a retention matrix, which sets out retention periods by information class, and which is supported by technology designed to survive the retention period.

3 The EU Data Protection Directive 1995 (Directive 95/46) has been implemented in each of the member countries of the EU. National legislation reflects national legal requirements and is usually in the national language (eg Greek in Cyprus, German in Germany) and entered into force at different times. In some countries, such as Germany and Austria, there is further data protection legislation at the local state level that implements the EU directive. All national legislation incorporates eight principles about the processing of personal information (information that enables a person to be personally identifiable) which are that it must be:

1. Fairly and lawfully processed;
2. Fairly and lawfully obtained;
3. Adequate, relevant and not excessive;

User breaches of retention requirements

Clearly, allowing individual users to determine when to destroy or delete their own email records is a prima facie breach of a company's legal record retention obligations.

Encouraging or allowing the creation of email archive files that don't align with the corporate data retention policy is a similar breach, exacerbated if they cannot be systematically backed up and their ongoing retention cannot be assured.

Conversely, organizations must be able to destroy data when they no longer need it or when it falls outside a mandated retention period. There are practical and commercial reasons for this: technology becomes obsolescent and the continuing cost of data storage needs to be controlled. This practical consideration has legal force in respect of individual data, which must be destroyed when the purpose for which it was collected is no longer valid.

Data Protection Act

European regulatory requirements go far beyond statutory and practical document retention periods. The European Data Protection Directive³ "ensures that organizations manage the personal information they hold in a sensible way. Organizations must keep the information accurate and up-to-date, they must only keep it for as long as needed for a specified purpose and they must keep it secure."⁴ These requirements apply specifically to any emails that contain information about individuals, and cover communications about recruitment, discipline, remuneration, incentivisation, including computer scoring, opinions, views and comments, however ill-informed. Sensitive data, information which deals with health, religion, and sexual orientation, must have a higher level of protection than other data.

It is an explicit requirement of the Seventh Principle of the EU Data Protection Directive that organizations take **"appropriate technical**

4. Accurate and up-to-date;
5. Not kept longer than necessary;
6. Processed only in accordance with the data subject's rights;
7. Kept safe and secure ("appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data")
8. Not transferred to a country outside the EU unless there is at least a similar level of data protection available there.

4 Data protection myths and realities, UK Information Commissioner's website,

and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

Rights of data subjects

Data confidentiality is an important principle of data protection regulations: personal data must not be accessible by anyone not authorized to view it. Simultaneously, organizations must protect the

“Seventh Principle compliance requires organizations to have a formal, central strategy for email capture, retention, storage, maintenance and eventual destruction.”

integrity of that data: in the UK, for instance, the Data Protection Act 1998 gives individuals (or ‘data subjects’) the right to find out what information is held about them by any organization, and to have inaccurate data amended or destroyed. Data subjects may take action

against, and receive compensation from, organizations that fail to respond within the allowed 40 days from the date of the request.

Organizations must identify, within the specified time limit, any information that they hold about a data subject and be able to delete any incorrect information – wherever it may be stored. Data availability, as a principle, must be built into the organization’s email management strategy. Those organizations that either, allow or encourage end users to create their own, local, email archives, are usually unable to respond to access requests within the time allowed or to amend or destroy ALL incorrect information.

Those organizations operating both inside and outside the EU have to meet additional data protection requirements.

Compliance with an entity’s own national version of the EU directive is usually adequate for compliance elsewhere in the EU. Organizations operating in North America may also be subject to the requirements of US legislation such as **HIPAA** (Health Insurance Portability and Accountability Act) and **GLBA** (Gramm-Leach-Bliley Act), or Canada’s **PIPEDA** (Personal Information Protection and Electronic Documents Act).

Human Rights

Meeting the requirements of the EU Data Protection Directive is further complicated by the **European Convention on Human Rights (‘ECHR’)**. This gives the citizens of member states a number of specific rights. Like the Data Protection directive, the ECHR has

been implemented differently in each national state. Article 8 includes the citizen’s right to respect for “his home and his correspondence,” and Article 10 says that everyone has “the right to freedom of expression.” Organizations are entitled to limit the exercise of these rights under specific circumstances and for appropriate reasons, such as preventing the misuse of organizational facilities or to protect the rights of other individuals. However, they cannot prevent any individual bringing a complaint that his human rights have been breached and this means that organizations must retain all the email information that might pertain to such a complaint.

Sectoral regulation

The EU Data Protection Directive applies to all organizations. Most organizations also have to deal with additional information-related regulations that are specific to their industry sector. The financial sector has to collect and retain information that demonstrates its compliance **with anti-money laundering regulations** as well as those regulations that require consumer-orientated financial services firms to prove they’ve taken appropriate steps to **‘know their clients’**. Professional firms (particularly lawyers and accountants) must also ‘know their clients’ and, in some jurisdictions, have specific responsibilities in relation to what they report about their clients to tax and other enforcement authorities. **Email records are an essential component of ‘know your client’ audit trails.**

Freedom of Information

UK Public sector organizations must comply with the **Freedom of Information Act 2000 (‘FOIA’)**. This act essentially gives interested members of the public the right to obtain answers to specific questions on areas (subject to some exemptions) that interest them and to do so within a specific period of time. Predicting exactly what sort of information may be required is impossible; what is possible, though, is the expectation that some of the information that may be required will be contained in email records. UK public sector organizations need to ensure that data is available when it needs to be; they cannot allow users to create their own archive files if they are to answer any search request they receive.

The FOIA also creates a specific criminal offence under its section 77. This **prohibits altering, defacing, erasing, destroying any record (including emails)** with the intention of preventing its disclosure. This means that public sector organizations that allow individuals to determine which emails they should destroy may, by default, be in breach of this section and liable for criminal sanction.

Internal control regulation

Companies listed on US stock exchanges, irrespective of where they are headquartered, are subject to the requirements of the Sarbanes-Oxley Act ('SOX'). These requirements extend to their subsidiaries and to supplier organizations responsible for significant components of the organization's activity, particularly outsourced suppliers.

Section 404 of SOX requires the directors, and their auditors, to each assess the effectiveness of the organization's internal

control structure, particularly with reference to preventing or detecting unauthorized transactions or the unauthorized use of the company's assets. In today's business world, email is the method by which such transactions and activities are

"Increasingly, email record control will be fundamental to European corporate governance and internal control structures."

most likely to be carried out. **Control of email records is therefore fundamental to SOX section-404 compliance.**

As Europe moves toward SOX-like corporate governance regimes, characterized by regulatory requirement and penalties rather than the UK's current 'comply or explain' approach, organizations must increasingly prepare to prove that their internal control structures can detect and prevent unauthorized transactions.

Financial regulation

The EU's **Markets in Financial Instruments Directive ('MiFID')**, due for implementation into the domestic law of EU member states by 31 January 2007, will have a significant impact on the record-keeping requirements of regulated financial services firms. While the detail of those requirements is not yet finalized, it will cover reporting information to customers, obtaining information from customers, customer agreements, management of conflicts of interest, compliance arrangements, and internal systems and controls. In each of these areas, email records will play a significant role in post-event demonstrations that the firm complied with the requirements of the directive. Investment firms across Europe must therefore ensure that **their MiFID compliance activity extends to email archiving and retrieval.**

Construction

Firms operating in the UK construction industry are subject to the Construction (Design and Management) Regulations which, in essence, require appropriate steps to be taken at all stages of the design and build process to avoid foreseeable risks to the health and safety of individuals, to combat such risks at source, and to give priority to measures that will protect individuals who may be affected by the building work including, for instance, maintenance contractors and cleaners.

Construction is a multi-disciplinary process and **compliance with the CDM regulations relies on the archive quality of meeting records and associated communication, most of which is in email format.**

Litigation Risk

While a demonstrated failure to meet regulatory compliance requirements may be embarrassing and commercially damaging for any organization, the potential impact of an inability to access relevant emails in respect of a law case can be catastrophic. The availability of the information may be as important to the organization as its integrity.

There will be times that an organization needs to demonstrate that it has followed its own procedures, or that the law has been fully applied. This may happen in employment law or Industrial Tribunal cases where, for instance, the organization is defending itself against charges of unfair dismissal or racial or sexual discrimination and it needs its email records to prove, conclusively, that every step followed in a particular case was objective, lawful and in line with its stated policies and procedures.

There will also be times when the organization needs to demonstrate, beyond a shadow of a doubt, what its intention was in the detail of a particular commercial contract, or that it took every step necessary to deliver against an agreed set of requirements, or that the real cause for a breakdown in a commercial relationship was entirely to do with the opposite side. In all these cases, email records will contain the crucial evidence on which such claims stand or fail. Any inability to identify and produce in court all the email evidence that supports the case will lead to a litigation failure.

Law courts increasingly recognize the evidential importance of email and are likely, where litigants fail to produce relevant email evidence within usually very short time scales, to authorize opposition lawyers to investigate the email archive in what is known as a 'fishing expedition'. Not only can this expose otherwise confidential information to unfriendly parties, it can also give them new and unexpected perspectives on the issues that they are pursuing.

From a practical, commercial perspective, organizations must be able to systematically, comprehensively and conclusively identify and produce all the emails that may be relevant to a particular case, and to do so within a time scale measured in days, not weeks.

Best-practice guidance

Organizations face a complex challenge in determining how best to approach their email management and archiving requirements. They need to:

- Minimize data storage requirements and costs; and
- Eliminate multiple, user-defined data-retention policies.

The market is full of competing products, which appear to meet some of the challenges outlined above, but most organizations find themselves assessing archiving solutions without clear guidance as to the most appropriate solution for their needs, or the extent to which their selection should favour one or other of the three issues identified above

While it is certain that no single email archiving product can, of itself, deliver regulatory compliance for any one organization, **there are proven steps that organizations can take to position themselves to meet current and future operational, regulatory and litigation-support requirements.**

ISO 17799

Internationally recognized best-practice guidance is provided by ISO/IEC 17799:2005, the international Code of Practice for organizational information security management systems. ISO 17799 is sector-neutral, technology-agnostic and vendor-independent. It deals with organizational systems, not product specifications. Developed over ten years, it contains latest international best practice recommendations, consolidated into a single coherent set of information security control recommendations.

At the heart of ISO 17799 is **the concept that information security requires the preservation of the confidentiality, availability and integrity of information.** ISO 17799 says that all appropriate steps should be taken to protect confidentiality, availability and integrity and that no one aspect of information security is any more important than any other. Information security is, from the viewpoint of the standard, a business enabler.

As a Code of Practice, ISO 17799 recommends that organizations should select controls on the basis of the board's assessment of the risk (both business and regulatory) that it faces, and its appetite for risk. Technology solutions should contribute directly to achieving the controls the board has identified as important. Critically, investment in a control should not exceed the likely cost of the potential harm arising from the risk to which it is related.

From the perspective of multiple, sometimes conflicting regulatory compliance requirements, any organization that implements international best-practice recommendations clearly places itself in a strong position to argue, in any court and under most circumstances, that it took the most appropriate action to meet its legal and governance obligations.

ISO/IEC 17799:2005

ISO 17799 recommends four general controls in respect of the business issues identified in this paper. These are:

10.5.1 Information backup: back-up copies of information should be taken and tested regularly in accordance with the agreed back-up policy;

10.8.4 Electronic messaging: information involved in electronic messaging should be appropriately protected;

15.1.3 Protection of organizational records: important records should be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements; and

15.1.4 Data protection and privacy of personal information: data protection and privacy should be ensured as required in relevant legislation, regulations and, if applicable, contractual clauses.

In addition, ISO 17799 provides guidance on other aspects of information security that have direct relevance and importance to email management, including information security policy, anti-malware controls, access control, business continuity and information security incident response. All of which should be considered when assessing email archiving and record management technologies.

For each of its clauses, ISO 17799 provides detail as to how it should be implemented. More importantly, **the standard makes clear that all the controls are important, and indicates that organizations should take appropriate steps to apply them all.**

ISO 17799 deals with the general security environment within which information is collected, stored, protected and made available. There is further, specific best-practice guidance available in respect of information archiving and electronic records management that should also be considered.

ISO 15489, the BSI Code of Practice and MoReq

In addition to the general control recommendations of ISO 17799, there are standards that deal specifically with record management.

ISO 15489

ISO/TR 15489:2001 is a two-part international standard that focuses specifically on records management for 'originating organizations', to help them ensure that adequate records, in all formats and media, are created, captured and managed.

BIP 0008

In parallel with the emergence of this international standard, the BSI in the UK developed BSI BIP 0008:2004 – A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. This is aligned with and underpins ISO 15489, so both guidance documents can be implemented in tandem.

BIP 0008 focuses, as does ISO 17799, on the confidentiality, availability and integrity of information. The overlap between BIP 0008, ISO 15489 and ISO 17799 enables organizations to use ISO 17799 for general controls and both BIP 0008 and ISO 15489 for the specific controls needed for their information archiving activity.

In the UK, public bodies are in any case required to seek conformance to the principles of BIP 0008, and it is applicable to organizations of all sizes, and in all sectors.

MoReq

The Model Requirements for the Management of Electronic Records (produced by Cornwell Management Consultants for the European Commission), provides an alternative model specification for Electronic Records Managements Systems (or 'ERMS') that is in line with ISO 15489 and BIP 0008.

MoReq recognizes that "documents made or received in the course of business become records" when they are captured by the organization's information systems. While **MoReq was written to cover all electronic records and is specifically applicable to email**.

MoReq provides detailed guidance around security controls (such as access control, backup and recovery from backup, controls over information transfer, authenticity and confidentiality, and audit), as well as detailed coverage of retention schedules, identifying the need for a review process prior to record-destruction that allows for an individual record's retention date to be changed. Transport, export or destruction of records should be controlled, and there should be an audit trail.

The use of metadata to enable the creation, management and use of electronic records is essential to any ERMS, and MoReq says that the metadata should be extracted automatically.

Conclusion

An email management, retention, maintenance and archiving solution should deliver against the general control requirements of ISO 17799 and the specific recommendations of ISO 15489, BIP 0008 and MoReq. An end-to-end solution should meet operational business needs, enable organizations to align their activities with regulatory compliance requirements, and ensure that they have the capability to provide adequate litigation support when needed.

Organizations that follow the best-practice guidance of ISO/IEC 17799:2005 at the general control level, and the specific recommendations of MoReq, ISO/TR 15489 and BIP0008, should select email archive solutions that deliver an end-to-end solution for their management of the operational, compliance and legal risks associated with email and digital information.

About IT Governance Ltd

IT Governance has been designing and successfully implementing cost-effective BS 7799 information security management systems since the standard was first released. The consultancy approaches IT governance, regulatory compliance and information security issues from a management perspective and is committed to engaging business leaders in developing and implementing information, ICT regulatory compliance and information security strategies that enable their businesses to compete effectively in the global information economy.

Alan Calder, author of "IT Governance - a Manager's Guide", is a founder director of IT Governance Ltd. He is a member of the DNV Certification Services Certification Committee, which certifies compliance with international standards including ISO27001/BS7799.

Alan works with a wide range of clients on IT governance and information security projects which include design, implementation and deployment of management systems and the development and writing of White Papers. He also speaks at seminars on IT governance, regulatory compliance and information security.

About ZANTAZ

ZANTAZ is the global leader in Information Retention and Disclosure Management solutions. ZANTAZ' solutions enable organizations to capture, preserve and access unstructured digital information – including email, IM, files, scanned documents, and other electronic records – and review and produce relevant documents in a manner that reduces operational risks and costs while complying with legal, regulatory and corporate policy requirements. ZANTAZ solutions are available as onsite software applications or on-demand hosted services, and include a broad set of professional services and integration support. ZANTAZ has over 600 customers, including many of the largest corporations, law firms and government agencies in the world. For more information, visit www.ZANTAZ.com or ring on +44 (0)207 3978 760.



For more information:

Visit www.zantaz.com

Or contact your ZANTAZ reseller partner

Global Offices

ZANTAZ, Inc.

Corporate Headquarters
5671 Gibraltar Drive

Pleasanton, CA 94588

Boston

399 Boylston Street
12th Floor

Boston, MA 02116

New York

230 Park Avenue
10th Floor

Suite 100, Room 15
New York, NY 10169

Canada

1600 Carling Avenue
Suite 800

Ottawa, ON K1Z 1G3
CANADA

London

St. Martin's House
16 St. Martin's le Grand

London, EC1A 4EN
UK