



Market Perspective Whitepaper
February 2007

Prevention v Post-Mortem

Regulatory Compliance for Senior Executives

> [orchestriawhitepaper](#)

MANAGING CONFLICTING TRENDS

Major organizations today are increasingly susceptible to public humiliation, legal proceedings, regulatory fines and the possible dismissal from the organization. At the very top there is a more threatening climate of personal accountability for senior management. This tension is the result of several powerful but conflicting trends: the relentless drive of technology in opening up business communications and the pressing need to control the content. The result is a new regulatory landscape for business operations. The implications are critical for today's senior executive. Now, more than ever, there is a need to identify and prioritize the key risks to corporate well-being, manage them at the highest level and implement effective solutions throughout the entire organization.

In the corporate landscape through which information not so much 'flows' as 'floods', the new workflow is unstructured with no well-defined management or control.

FREEDOM AND CONTROL

At the center of the debate is the changing nature of electronic action (message, web and file activity) within and between financial business institutions. There is no doubt that the modern business information model has 'freedoms' not possible a decade ago. A cliché of networked corporations is that the flow of information through a business is its lifeblood. A fundamental assumption for business is that the nature of markets, stock exchanges and communications in general is reducing space and time so that interaction is virtually instantaneous. These and other factors are refining, expanding and developing new challenges for business growth and profitability. Traditionally this information was managed and monitored by highly centralized IT departments with access stringently controlled. The ability to communicate business information was strictly limited to corporate need and company policies were easy to enforce. But this new workflow is largely unstructured with no well-defined management or control. Massive investment in networks, local and remote and the availability of PCs no longer dependent on centralized mainframes, has expanded the possibilities of information flow within and between organizations. The emergence of the Internet as a model of how information can be exchanged has led to a quantum leap in corporate systems: Intranets and extranets are models that have swept away the older, centralized information management systems. Powerful mobile devices such as laptops, cell phones, mobile devices, corporate VPNs and high bandwidth availability from the home have each contributed to and fuelled the growth of universal access. All these elements have deluged the corporate landscape with devices and alternative channels through which information not so much 'flows' as 'floods'.

The importance of this business freedom is irrefutable. But a balance is required to make accountable the power and influence of the chief product of this freedom - information. At the highest levels of corporate activity is a public determination to insist on effective control. The innermost, private nature of public corporate behavior has been exposed and found wanting.

Political consternation has translated into the regulation of the nature and manner in which a company acquires, exchanges and disposes of information and its core wealth. The bodies that manage regulations define how corporations meet, and demonstrate that they have met, their responsibilities. The technologies that have, by and large, enabled this freedom have now to be used to curtail and control corporate behavior. Ironically this free-flowing information is both a great ally of business life and also the unwitting instrument of corporate exposure: the email that closes a deal provides enough evidence to condemn a company. The dilemma for the modern business is how to balance operational freedom and necessary regulatory control. This dilemma is a tension that runs through today's corporations, and carries with it a loss of innocence about what technology can do. For the company the penalties for non-compliance are significant and for senior executives the personal cost can be devastating.

UNSTRUCTURED COMMUNICATIONS IS THE NEW WORKFLOW

The benefits of the new landscape, its fluidity, flexibility and relentless drive to open-up and share information are many. Trends in technology have worked to empower the user, break down borders and ultimately enable organizations to operate in real-time, to act on impulse and to leverage the flow of real-time information. But as with all things there is a price. Many business users often fail to understand the implications of these impulsive, 'informal' interactions. The proliferation of 'unstructured communications' such as email, the Web and Instant Messaging (IM), and file activity, is a double-edged sword. Material such as sensitive, financial and business data, IP and PII information is now exposed through uncontrolled channels. The pragmatic interactions and discussions of any active organization, raw data, 'unframed' information, private memos, hearsay and verbal communications, previously managed centrally, are now packaged locally in emails and through IM channels, distributed to multiple destinations, carried along by the powerful currents of this flow. The ability to monitor and control this information before it is exposed to the world at large is slipping through the fingers of corporate managers. Emails and archived files are now regularly produced in court hearings for litigation support in cases of fraud, insider trading, coercion, harassment and industrial espionage. For many organizations, unstructured electronic activity is an accident waiting to happen. This is illustrated by a few high profile examples. The now-defunct accounting firm Arthur Andersen was judged guilty of misconduct in the Enron case on the strength of one email. Investment banks, Credit Suisse First Boston and Merrill Lynch, have both had internal emails used in evidence against them in SEC malpractice investigations. The scale of this challenge is daunting. In 2002, IDC forecast that "Over six billion business emails will be sent each day". Today, that number is dwarfed.

Unstructured communications is an accident waiting to happen.

The dilemma is how to balance operational freedom with regulatory

These recent high profile cases have resulted in a loss of public confidence in corporate governance and the economy as a whole. They have also served as the driver for a counter trend towards stricter regulation with the goal of re-establishing corporate integrity and public trust. The Sarbanes-Oxley Corporate Responsibility Act (SOX) provides the fundamentals for corporate disclosure by addressing controls absent from corporate accounting and according to Harvey Goldschmid, a commissioner at SEC, resulted in reforms that might not have happened without Enron's collapse. Suddenly email is a significant arena for investigative interest. SEC has indicated that the quantity of incriminating emails among those reviewed during investigations has been an eye-opener for its staff. In October 2003, in one investigation evidence was unearthed of senior management instructing subordinates to delete email in connection with violations. What alarmed investigators was the way some fund employees sought to get around SEC surveillance by using other means of communication. It added that as part of routine inspection it may need to read emails across all areas of the business not limiting themselves to the documents identified by SEC rules. In some instances, SEC staff has asked for not just emails in the subject areas but everything in the archive and on servers if there are suspicions of a cover-up.

What is transparently true is that governments and industry regulators across the world are tightening up on the way organizations are permitted to operate.

TIGHTER REGULATION AND REFORM

What is transparently true is that governments and industry regulators across the world are tightening up on the way organizations are permitted to operate. US legislation has appeared in the form of the Sarbanes-Oxley Corporate Responsibility Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA) as well as regulations from the Securities and Exchange Commission (SEC) and the National Association of Securities Dealers (NASD). In the UK, industry guidelines include those published by the Financial Services Authority (FSA) and the 1999 Turnbull Report with its associated UK Code of Conduct, published by the Institute of Chartered Accountants in England and Wales (ICAEW).

The META Group surveyed CFOs and IT personnel regarding the Sarbanes-Oxley Act (SOX) and its impact on current corporate IT initiatives, project prioritization, and funding. The significance of corporate financial systems in SOX compliance became very clear. The results of the META Group survey found that for US public companies, the reporting requirements of Section 404 of the Act spurred to major project investment, taking up significant senior executive time and operational resources throughout the organization. Section 404 required that public companies demonstrate an understanding of the needs to improve financial reporting, document this and initiate projects to implement improved internal controls. Internal financial processes must be certified, and external auditors must identify the status of such a process and its likelihood of completion during a year-end audit.

Above all this hangs a Sword of Damocles in the form of severe penalties from a negative result of an SEC inquiry

As a consequence many companies are now analyzing, end-to-end, their financial processes through to the eventual reports delivered on SEC statements, such as 10-K and 10-Q. The survey found that many Global 2000 firms are concerned that their existing practices do not match the financial management processes defined by SOX. These companies implied their financial systems do not allow the degree of consolidation required and just under half indicated this was an area they had to address urgently. They believe they are in serious danger of non-compliance given the time-scales and the amount of internal process re-work. There are other challenges: in order to fund these activities companies will have to prioritize other projects. . It's not just in the US that the effect of regulation is being felt. Unlike in the US, the percentage of financial institutions using technology to ensure compliance over email, Web and file activity is significantly lower in the less regulated UK. Yet many of these companies listed in the US are expected to conform to laws such as Sarbanes-Oxley and the guidelines from regulatory bodies such as SEC and the National Association of Securities Dealers (NASD). A recent survey found that 56 per cent of respondents have no technology in place to manage and monitor the content and context of employee emails, Webmail and Instant Messages. It seems that compliance officers in these companies have no way of knowing when an employee is sending a communication that breaches regulations such as the FSA Code of Conduct, leaving those companies wide open to regulators' fines, or worse.

All areas of the finance industry are affected by this surge in regulation. Although the bulk of regulation applies to public companies the net is likely to widen. In an effort to pursue mutual fund trading abuses the SEC and NASD are currently bringing disciplinary actions against at least twenty firms for 'breakpoint' violations. Some firms have displayed evidence of a systemic weakness where breakpoints were not being properly monitored. Mutual fund companies and brokerages are required to store documents in a manner that is easy to retrieve by regulators. Yet again unstructured communications presents the regulators with opportunities to address violations. Ironically, much of the malpractice is recorded. It is a question of knowing where to look for the information and how easily it is accessed. Given the volumes of data and the real-time nature of the activities, speed of action depends on effective access. Elliot Spitzer, former New York attorney general, used emails and trading records to build cases against several companies. In one such classic example, Spitzer was able to corroborate suspicions of violation because of an email that confirmed a deal. Efforts to pre-empt future errors in sales load calculations are based on co-operation between mutual fund, Broker Dealer companies and NASD. It is likely to lead to possible operational enhancements, disclosure requirements and even further regulatory changes.

THE COST IMPACT

Across the industry the impact of current regulations and those in the pipeline on business planning and costing is variable, and it is not only the finance company that pays a price. Audit firms, for example, may no longer provide other services to the companies they audit. Investment bankers are no longer able to influence reports produced by the bank's research division. Regulations are tightening in many other areas too, from the selling of mortgages and pensions across industries to the transmission of confidential patient data. But it is the cost that concentrates the mind of the board. New projects have to be funded and budgets stretched or created to accommodate cross-discipline programs

Executives are exposed to unprecedented levels of scrutiny and personal accountability.

EXECUTIVE RESPONSIBILITY

What of the senior executive perspective on this, and how far does responsibility spread within the organization? As the corporate governance debate continues to focus on legislative policy to deter fraud and set the highest standards to date for public companies and their auditors, organizations can no longer cloud the sources of authorship, attribution or responsibility. This leaves executives exposed to unprecedented levels of scrutiny and personal accountability as loose statements of integrity are no longer acceptable. Companies must articulate their leadership and commitment to corporate governance and at the same time demonstrate the policies and processes behind their communications, research and handling of customer data. The C-level executive of every company listed on a US stock exchange - which includes several hundred major European companies - must now swear that any financial disclosure his or her company makes is full and accurate. Further, the SOX legislation also makes a distinction between an executive who "unknowingly" signs off inaccurate financial statements and one who does so "willfully and knowingly".

While much of the regulatory effort is now taken up with inspecting information itself, scrutiny now includes how it is communicated within an organization. The focus is on dialog. NASD is undertaking pilot projects and incorporating lessons in future regulations. It now inspects Broker and Dealer compliance departments to assess how well they communicate with other parts of their company including the CEO. These inspections or 'compliance examinations' are initiated where NASD finds internal business communications to be poor. In a parallel activity, SEC may recommend that primary compliance oversight at a company can be designated to more than one officer in a bid to spread the load of responsibility especially in specialized areas, such as money laundering and proxy voting. This extends to the introduction of consultants to double-check compliance.

From this it is clear that levels of responsibility stretch down into an organization, the implied spread of responsibility following the flow of information. But definition is everything in the legal maze of compliance. It is

In the regulatory world, real accountability settles on the senior executive.

being claimed that the NASD compliance certification proposal may expose compliance officers to liability from private lawsuits and not just regulators. Some of the proposals add to the exposure by asking them to certify procedures in areas of business in which they lack expertise. There are roles and responsibilities that would benefit from further clarification. Further down the chain it is now claimed that Investment Adviser SEC compliance certification may open the company to increased fraud liability. David Tittsworth, ICAA executive director has been quoted as noting that legally 'an aggressive SEC' would be able to define any violation as fraud. With so much depending on fine definitions of role and responsibility the line between violation and fraud can be a thin one and while many SEC infringements are not serious enough to warrant penalties, fraud is a much more serious charge.

In the regulatory world, real accountability settles on the senior executives. It is they who are held to be responsible for company failings.. After the disasters of a self-regulated past it was felt senior managers had to be made 'properly' accountable. The Act made it clear that 'Controlled Functions' in regulated companies could only be carried out by approved people, including senior management. A key principle is 'compliance with regulatory requirements'. Those exerting significant influence within a regulated entity must take responsible steps to ensure there are guidelines and rules and that these are implemented within their company. Ambiguous guidelines are a major concern, a situation complicated by compliance staff not experienced in everyday business and not best equipped to spot issues as they arise. These are indeed uncertain times for senior managers under pressure to offer staff greater autonomy yet constrained to ensure control. There is no defense relating to lack of knowledge about rules, regulations or responsibilities in the eyes of the regulator. The chain of responsibility goes up, escalated ultimately to the board. And how is all this to be monitored? Most of the reporting on violations will be undertaken by company lawyers. Section 307 of SOX addresses the standard of professional conduct for lawyers and encompasses SEC attorney-conduct rules governing how legal staff escalate violation issues to senior executives. Lawyers are required to climb the ladder of responsibility depending on responses received, all the way to the CEO or board of directors. There is a broad discretion as to how they report violations against their superiors but in uncertain times some subordinate attorneys may play safe and report everything they see. There are concerns on what should be reported since this may be a recipe for over-reporting. Further, tensions can arise from responsibilities to report on a board that is dead set on violating. Ultimately it is the senior executive that is most exposed in this new climate, and it is in his or her best interests to plan an effective compliance enforcement regime.

Every power-user, every call-centre employee has the potential to cause damage to the corporate good.

SOLUTIONS - PREVENTION OR POST-MORTEM?

While CFOs, compliance officers and corporate lawyers are busy putting internal policies in place to ensure that they comply with regulations, many are discovering that policy enforcement has a serious Achilles' heel. Although information boundaries, both internal and external, must be recognized and reinforced to ensure the sharing of sensitive research or customer data is limited, unstructured communications, as the new workflow, constantly redefines itself to meet sudden and rapid changes in the market, flowing in new directions with new imperatives for business survival and growth. Businesses are increasingly aware that even seemingly informal recommendations made over unstructured forms of electronic communication need to be effectively managed, monitored and archived for possible inspection by regulators. Surveys have unearthed significant increases in the use of electronic records by financial firms, largely as the result of regulations such as SOX. In one survey over half of the respondents, of which three-quarters were Fortune 100 companies, indicated SOX as the reason for changing to electronic records. The knock-on effect is to further drive a trend towards storage and retrieval and monitoring led by compliance officers. But the devolution of computing power to the desktop while boosting employee productivity, also presents a serious risk.

The carefully constructed working practices and processes of the past have been giving way to flexible, 'empowered' approaches where individual employees are empowered to shape a solution for a client or customer. All the while business time-scales are shortening to 'real-time'. Without 'real-time' reflexes corporate enterprises suffer and fall behind. Yet every power user in the organization, every call-center employee has the potential to cause damage to the corporate good. Employees have the power to divulge information and make promises on the company's behalf entirely without management visibility or control, often leading to knowing or unknowing violations of corporate policy, leaks of confidential information and breaches of financial or industry regulation. So the challenge is how to manage the control needed to ensure the company prospers and meets regulatory obligations.

There are solutions that claim to offer real-time intervention that work on the principle of blocking in the first instance with a follow up action of 'review and release'. Electronic message and file archiving and retrieval systems launched to meet regulatory requirements, variously billed as compliance tools, speed up searches, provide audit centers and so on. These tools may address the interests of some compliance officers seeking certification under SEC and NASD rules, but they do not address the critical issues of violation itself. The 'block-review-release' approach is very intrusive for day-to-day workflow resulting in considerable disruption of already time-critical processes. It is potentially very labor intensive at a time when organizations are seeking to gain critical competitive advantage from automated systems. In reality a purely manual system is unwieldy. It is focused on archiving

What is required is a system that interacts with user in real-time and manages risk at source, on the desktop.

huge amounts of data and information, accumulating reviewable data somewhere along the line between the company user and his or her destination. It requires constant review of massive flows of information and a set of policies that somehow encompass all the possibilities of non-compliance to regulations that are, at times, vaguely expressed and legally loosely defined. It is a system prone to error.

Many companies and government departments have invested, or are considering investing, in email, Web and file monitoring software. However, since most software packages of this type only address part of the problem they cannot prevent a user from conducting a non-compliant electronic activity: they can only identify retrospectively that such an email, web or file activity has been occurred. Paying lip service to regulatory compliance by instituting a process that is demonstrably in compliance doesn't in itself assure the senior executive that the company will not make these mistakes. This 'post-mortem' approach is useful in the provision of an audit trail, but does nothing to prevent the breach occurring in the first place. Once uncovered by the regulator it opens up the paper chase into the heart of the business. The perspective of the CEO is of the one who has to sign up to a consolidated financial view of the organization and commit to that view. In this context, the senior executive needs all the help he or she can get in ensuring such critical mistakes are not made in the first place.

A more elegant approach is called for, one that intervenes but does not interrupt communication across diverse mediums. What is required in order to control more effectively the flow of email, web or file activities – both from the company's servers, gateways and endpoint – is a software system that interacts with the user and can intervene in real-time, i.e. in between the user hitting the "send, upload or save" button and the activity becoming a discoverable event. It requires a solution that manages the risk at source, distinguishing potentially damaging activity from the permissible. A solution that intelligently understands the content of each electronic action, determines its nature and purpose in real-time and allows those action which adhere to corporate or regulatory policy to continue without operational detour. It is one that captures non-compliant events before they are considered discoverable events. What is needed is a system that is based on 'prevention'. This is the essence of Orchestria's Intelligent Electronic Control (IEC) software, which is already being used by a number of Global 1000 corporations in order to minimize non-compliant activity.

IEC: THE ROUTE TO CORPORATE COMPLIANCE

With technology that provides unprecedented levels of real-time visibility and control of all electronic communications, Orchestria's intelligent control layer works by applying specific and explanatory policy at the point of each interaction. This means that non-compliant events, such as information boundary breaches, document-sharing violations or inappropriate disclosures are determined and filtered as they occur and before they are sent. These front-end functions of active, real-time, monitoring and

intervention are twinned with intelligent and efficient archiving after the electronic action.

IEC has been deployed by some of the world's largest corporations, including Wall Street banks. The technology analyzes content, context and people; enforces corporate policy; lowers risk; eliminates unauthorized data loss and ensures regulatory compliance. This solution ensures policies - legal, regulatory and corporate - are enforced as events take place and not after a violation of an established policy. This gives organizations an active enterprise solution that can interact with the user before an email, Web or file activity strays outside a given company's corporate policy, defined process or governing regulation.

IEC operates 'actively' and continually throughout all electronic action workflow, yet is largely invisible to the user. IEC works by intervening in real-time, monitoring and controlling all messaging, Web and file activity traffic at the point of interaction. This preventative approach effectively filters all files before they are archived and retains according to content.

IEC intelligently classifies and indexes every event in real-time, understanding the nature, purpose and context. It threads all activity to provide the most advanced audit trail and retrieval capabilities. For **supervisory consoles** IECs consoles provide customizable views, giving real-time visibility of all relevant data. This ability to see detailed and summarized interactions in real-time dramatically reduces the time and costs associated with compliance activity. Additionally, with no limitation on the number of supervisory consoles, team leaders and executives may view micro-to-macro detail.

Loss of license, large financial penalties, jail terms and high profile coverage are very real threats. The only real **insurance** is IEC. The preventative rather than post-mortem approach offers the only real insurance to executives, reputation, shareholders and Intellectual Property.

IECs lifecycle management for all 'unstructured' communication establishes order from chaos. It enables corporations to build effective processes, with rapid implementation, in the areas of auditing, archiving, retrieval, retention and general policy management for all electronic action.

IEC notifies all personnel such as traders, brokers and researchers of any policy breach by dynamic screen pop-ups that explain the offending item. This means IEC is able to modify behavior by explaining the cause and recommended action at the point of every offending interaction. In effect users are trained in real-time whilst generating revenue.

By implementing such a pro-active solution based on prevention rather than re-actively trying to assess violations and by using tools that minimize cost and process overhead, the organization is well positioned to respond to existing and future regulations.

SUMMARY

As industry regulation grows tighter, compliance is becoming harder to manage, yet the growth in the unsupervised use of email, the Web and Instant Messaging for business communications is explosive. Nevertheless, the business benefits of such an information flow are irrefutable. Market-proven with implementation sites that include a number of the world's leading investment banks, Orchestria has developed a solution that uniquely enables organizations to identify risky communications before they are sent, enabling the organization to lock the stable door while the horse is still safely inside.

For the senior executive seeking to mitigate the risks associated with compliance breaches, leaked information and the loss of intellectual property, there is a strong requirement for a strategy based on the prevention of regulatory violation. The case for Intelligent Electronic Control is paramount for every company working through this change. The costs of complying with current regulations are high. Yet for years to come, the cost of not implementing an effective solution for both the company and the senior executive could be significantly higher.