

This paper is one of a four-part series of COLT and IDG white papers addressing the most pressing issues facing CIOs of major European organisations. [include link to list of concerns].

The need to play a more strategic role in business without raising capital expenditure has led many CIOs to embrace selective outsourcing solutions, in a bid to **optimise IT resources** (url).

Burgeoning European regulations and compliance requirements have also led C-level decision makers to seek **risk mitigation** (url) strategies.

Meanwhile, the need to address demand for **flexible working** (url) from customers, employees and dynamic market requirements has persuaded many large organisations to consider managed services from a third party IT and telecoms partner.

The fourth and final paper addresses the perennial need to achieve **business efficiency** (url) brought sharply into focus by recent economic conditions.

# RISK MITIGATION

## WHY EUROSOX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

### Contents

Executive summary	2
Introduction	3
The business and regulatory challenge	4
The compliance landscape	5–7
The key to successful implementation	8–9
Choosing the right partner	10
Conclusion and benefits	11

in association with



## RISK MITIGATION

WHY EUROSX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

### EXECUTIVE SUMMARY

Ensuring compliance with European regulations and standards isn't just a question of 'doing the right thing' – it's a fundamental part of risk mitigation. Compliance is as much about being in control of your IT assets and ensuring that they work properly as it is about legal issues. By 'doing the right thing' CIOs are also doing the profitable thing, embracing compliance as a business opportunity rather than an organisational chore.

However confusion reigns in the face of an increasingly complex European regulatory framework. There are thought to be more than 180 legal regulations facing today's CIOs – depending on the business sector the number might be even higher.

A set of landmark EU directives on corporate responsibility, dubbed EuroSOX, are of particular concern. These Directives are due to start being passed into law by member states in summer 2008, and CIOs are fielding questions about how they might affect the overall compliance strategy of their organisations. How does EuroSOX differ from other regulatory legislation? Is it simply a European version of America's

Sarbanes Oxley and if not, in what way is it different? And where do standards and frameworks such as ISO and ITIL fit in with current and impending European legislation?

Industry experts have already highlighted their concerns about the upcoming directives. "EuroSOX is intended to harmonise existing laws but a lack of clarity compounded by 25 translated versions and different interpretations of auditing rules could confuse the true meaning of the legislation and jeopardise its positive effect on internal risks and controls," says Andy Jones, senior research consultant at the Information Security Forum (ISF).

With a particular emphasis on EuroSOX, this paper will describe the current European compliance landscape, outlining key standards and frameworks along the way. We will also offer a roadmap on how best to navigate the regulatory minefield.

Finally we will show how partnering with the right IT and telecoms provider can turn the process of compliance from a technical and bureaucratic burden into a business opportunity.

### WHAT IS COMPLIANCE REGULATION?

Regulatory requirements focus on establishing appropriate systems and processes to mitigate risks for the enterprise and to cater for transparent and traceable business processes. This is designed to ensure the confidentiality, integrity and availability of electronically-held information. Regulatory requirements also focus on keeping personal data confidential.

Regulations describe what *should* be done, but not *how*.

Executives can be held personally responsible for failing to comply with legal regulations and punished with financial penalties and prison sentences.

## INTRODUCTION

Exact legal guidance on what constitutes compliance is hard to come by, as regulatory requirements continue to evolve. Increasingly, these laws have subtle but varying interpretations from country to country, creating additional complications for organisations with a pan-European footprint. In short regulations describe what *should* be done but not *how*.

CIOs have been left on their own to work out how best to meet compliance requirements. To add insult to injury, they have to do work in an uncertain compliance environment where success goes largely unnoticed but the penalties for failure are only too obvious.

Well before EuroSOX, European regulations were strict. However they were also well understood and firmly established, allowing organisations to respond on a law-by-law basis. This was a perfectly logical approach, where companies shared a common understanding of the jurisdictions within which they could operate.

The past decade has witnessed a radical change in Europe's regulatory landscape, with the introduction of new regimes such as Basel II, creating a tougher, more complex environment – one that scrutinizes what you do, how you do it, and how you can vouch for it.

As CIOs have grappled with changing compliance-related legislation, they have also been faced with threats to their information assets from within their organisations. In addition, the arrival of rapidly mutating viruses and malware have exposed the technical vulnerabilities of IT systems, while procedural loopholes and the incompetence or lack of training of employees have put human fallibility in the spotlight more than ever before.

Simply put, your data and systems must be safeguarded through proven processes not just to protect you from litigation of all kinds, but because they are essential to the prosperity of your business and ongoing shareholder confidence.

### WHAT IS EUROSOX?

Otherwise known as European Sarbanes Oxley, EuroSOX is a set of landmark EU directives on corporate financial responsibility, due to start being passed into law by member states this summer.

The directives are designed to enforce financial transparency and prevent market abuse.

Directors must be able to disclose reports that reflect a 'true picture' for their company's situation.

## THE BUSINESS AND REGULATORY CHALLENGE

Onerous fines, brand damage and the outside possibility of a prison term for senior executives are outcomes that every organisation wants to steer clear of. But forward-thinking organisations want to do more than achieve the bare minimum of avoiding these worst-case scenarios: they want to ensure that in addressing compliance issues, the cure isn't worse than the disease.

In drawing up a compliance strategy, CIOs face the following challenges and considerations:

- Immense confusion over the impending EU EuroSOX directives, with translation issues and re-interpretations a particular cause for concern. Just as major organisations across Europe were coming to terms with existing corporate governance legislation such as Basel II, a new set of directives are causing widespread concern for CIOs.
- The threat of financial penalties and prison sentences (executives can be held personally responsible) for failing to comply with legal regulations.
- Beyond fines and legal bills, organisations found to be non-compliant may face revenue losses brought on by investor and customer confidence issues.
- Potential long-term brand damage, with public image negatively impacted after compliance breaches.
- Heightened media and regulatory attention to the subject of compliance following recent data debacles by government departments in the UK and other highly publicised cases across Europe. Scandals involving Skandia in Sweden, Spain's Afinsa, Parmalat in Italy and Germany's Siemens, mean regulators – and the auditors who work for them – need to be seen to be effective.
- Suppliers and stakeholders may distance themselves from organisations that fail to comply, fearing "guilt by association". This makes access to and cost of capital a problematic issue, especially as the effects of the credit crunch begin to make themselves felt.
- A bewildering and increasing array of 'compliance-friendly' vendors offering 'silver bullet' solutions.
- The number and nature of regulations will only continue to increase and become more complex.

"The degree to which these laws will be enforced by EU member states for the deadline this summer is currently unclear, but an aggressive approach to auditing and compliance could put a lot of pressure on information security departments and budgets."

Andy Jones, senior research consultant at the Information Security Forum

## RISK MITIGATION

WHY EUROSUX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

## THE COMPLIANCE LANDSCAPE

### EuroSOX

Of all the regulatory framework currently faced by CIOs the most talked about is EuroSOX, a set of European Union directives on corporate governance due to start being passed into law by member states this summer.

The origins of EuroSOX lie across the Atlantic in scandals that rocked US financial community and had repercussions far beyond. Ever since the Enron accounting scandals of 2001, a global spotlight has been trained on publicly traded companies forcing them to address the demanding requirements of demonstrating diligent corporate financial responsibility.

### Here comes the SOX

The fall out from the Enron, Tyco and WorldCom scandals ushered in the Sarbanes Oxley (SOX) Act of 2002 in the US, and set out to create new, robust standards in accounting and financial reporting for any company trading publicly on the US financial markets. With its 11 titles, SOX pinpointed a raft of additional corporate board responsibilities, addressing the way companies store and re-use data and imposing criminal penalties for negligence.

Europe's version of SOX is now waiting enactment. The European Union's corporate governance

directives, commonly known as EuroSOX, comprise a raft of measures that will collectively provide a regulatory framework for monitoring corporate financial responsibility across companies listed on European exchanges.

Europe itself has not been immune to financial irregularities of its own. Corporate misconduct involving Skandia in Sweden, Spain's Afinsa, Parmalat in Italy and Germany's Siemens, are forcing major European companies to grapple with the directives that form the basis for EuroSOX.

### What the directives say

The new directives require companies publicly traded on EU exchanges to disclose an independent chapter in their annual reports detailing management responsibilities. The disclosure must contain information and methods with regards to:

- Principle elements of the risk management system
- Principle elements in implementing internal controls initiatives
- Exemptions related to national regulations
- Description of the corporate governance codex

Prior to the arrival of EuroSOX, CIOs were faced with compliance issues relating to hard-hitting legislation. They include:

**Sarbanes Oxley:** Aims to improve quality and transparency in financial reporting, auditing and accounting practices.

**Basel II:** Promotes safety and soundness in the financial system by allocating capital in banking organisations to reflect risk more accurately. Banks should demonstrate a keen awareness of the need to measure, monitor and control credit risk as well as being able to show they hold adequate capital against these risks and that they are adequately compensated for risks incurred.

(continued page 7)

## RISK MITIGATION

WHY EUROSUX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

Companies must also disclose information on established systems and processes they have in place to mitigate risks and control initiatives. In addition EuroSOX requires that any new business created either through acquisition or merger should be able to show auditors consolidated accounts within a month of joining forces.

As yet, there is no sign of European legislators insisting on a full certification from external auditors for all publicly trading companies. However, management should be able to disclose a report that reflects a 'true picture' of their company's situation.

### Lost in translation

Already, however, alarm bells are ringing with industry experts pointing to the additional challenges faced by multinational companies when dealing with EuroSOX.

Each European state will have to interpret and translate the set of directives that comprise EuroSOX into 25 different language versions, leading to potential divergences of law between the different member states.

And for major European companies that means addressing different compliance regimes for every state in which they do business.

"EuroSOX is intended to harmonise existing laws but a lack of clarity compounded by 25 translated versions and different interpretations of auditing rules could confuse the true meaning of the legislation and jeopardise its positive effect on internal risks and controls," warns Andy Jones, senior research consultant at the Information Security Forum (ISF).

"The degree to which these laws will be enforced by EU member states for the deadline this summer is currently unclear, but an aggressive approach to auditing and compliance could put a lot of pressure on information security departments and budgets."

According to the ISF, the issue surrounding the interpretation of EuroSOX is further complicated by erroneous direct comparisons to the US Sarbanes Oxley Act, often fuelled by misinformed reports in the press.

(continued from page 6)

Companies without sound IT infrastructure systems in place run a high risk of failing to meet their obligations in accordance with agreed terms. This will make credit for these companies more expensive, since the costs are included in their risk premium which is part of the borrower's credit payment.

## RISK MITIGATION

WHY EUROSOX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

While there are undoubtedly a number of superficial similarities, they are outweighed by the significant differences. Sarbanes Oxley created whistle-blowing processes; addressed identity fraud; and set in place greater corporate governance responsibilities and high penalties for breaching them.

Few of these terms feature as part of EuroSOX, which is aimed at monitoring corporate governance, rather than policing it with a heavy hand.

According to Jones, the expense and disruption caused by the draconian way in which SOX was implemented could lead to a more cautious and drawn out approach from European legislators.

"While compliance is being driven at the highest level in most organisations, the implementation

of the Sarbanes Oxley Act both in the US and Europe has proved over-burdensome and costly," says Jones. "It is possible that some of this experience may mean that EuroSOX may be implemented more carefully and slowly."

### No test cases

With the directives yet to be implemented, there is as yet no tested case law and proven compliance methodologies against which CIOs can tailor their efforts to comply with EuroSOX.

However, despite the challenges discussed above and the uncertainty surrounding the new directives, all is not lost. A strategy that combines the right technology partner with security controls that ensure correct procedures to account for human behaviour is the first step towards effective compliance.

## STANDARDS AND FRAMEWORKS

Unlike legislation such as Sarbanes Oxley and Basel II, standards and frameworks are not obligatory. They exist to help ensure best practice for IT and business processes.

### ISO 27001

Part of a growing family of standards, ISO 27001 certification is optional (unless mandated by the organisation's stakeholders).

It lists a total of 133 controls in 11 information security areas, including: security policy; organisation of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition; development and maintenance; information security incident management; business continuity management; and compliance.

*Ref (1) Source, IDC Worldwide Security Compliance and Control 2006–2010 Forecast and Analysis: Going Beyond Compliance to Proactive Risk Management, September, 2006*

## RISK MITIGATION

WHY EUROSUX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

## THE KEY TO SUCCESSFUL IMPLEMENTATION

Building compliance into day-to-day business procedures can help you improve internal controls and identify opportunities to enhance existing work processes.

It can help you address the *real* risks to your business, often somewhat mundane in nature, usually caused by mistakes from people inside and outside your organisation.

By far the most common threats are caused by human action (or inaction) in the form of crime and error. An IDC survey (1) showed that the most dangerous threats come from unintentional employee mistakes combined with threats from hackers launching denial of service attacks, malware, spam and spyware.

The dangers of stolen or misplaced data also came high on the list. The recent damage done to the British Government in the wake of repeated data losses (all through incompetence) shows that no one is immune no matter how big they are.

The following six-point guidelines can help ensure successful compliance:

### People and processes

- Industry-leading products and technologies may provide the essential building blocks for risk mitigation, but the plan won't be effective without the implementation of rigorous procedures by well-drilled staff. It is important not to overlook everyday procedures that address well-known security threats, such as virus attacks or the inevitability of human error. Essential processes include: risk assessment for key assets; disaster recovery scenario planning; simulation and systems testing; and regular communications to employees.

### Regular training

- Employees need to know who should operate the appropriate technology and how, what to do should any aspect of the plan fail to work, and where they should go if they require further information. Extensive training is critical to ensure that human-driven errors, including failure to notify the right stakeholders or sending incorrect messages, are reduced to a minimum.

## ITIL

The ITIL framework is the most widely used IT framework in the world.

It comprises a series of 10 stripped-down, best-practice IT frameworks which apply to all organisations, regardless of size, scale or business.

Version 3 was released in May 2007 by the ITIL Certification Management Board and has refocused the framework to address maintenance and creation of IT and business processes.

The ISO standards and ITIL practices are the most commonly used by companies that strive to be in compliance.

## RISK MITIGATION

WHY EUROSUX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

### Data classification

- Classifying data according to its sensitivity and applying appropriate controls are the first steps to safeguarding the integrity of your customer data. The policy should include a data security plan that addresses the foreseeable risks to the integrity of the information maintained on your organisation's systems. With your data successfully classified and potential data risks targeted, identify the systems that manage this data for a more detailed risk analysis.

### Role-based permissions

- Establishing a role-based permissions policy can help ensure users only access the data they need according to the job they do. People can't lose or steal data they can't access. By imposing restrictions on downloading and copying personal information, you can protect your organisation from data being stolen by employees when they leave.

### Recording threats and attacks

- When have your systems been hacked and were they successful?

Did it affect customer data and, if so, how many customers were involved? In which of the European countries you operate in did the attacks occur? Bear in mind that even unsuccessful attacks may have to be disclosed, so your intrusion detection and prevention systems need to be able to create reliable records to prove their (and your) effectiveness.

### Appoint a chief privacy officer

- The role of the chief privacy officer (CPO) is to establish and oversee privacy policies to protect data for both customers and employees. A CPO can provide you with an official in-house compliance expert, chairing privacy discussions and formulating policies for managing incidents and achieving company-wide security awareness.

Taking a constructive view of dealing with compliance can help you ensure you are prepared for the risks facing your company's brand, reputation, assets and revenue streams. It can also improve your business processes, delivering real benefits to the bottom line not only during and after a crisis, but before it ever happens.

## COBIT

COBIT is an internationally accepted set of guidance materials for IT governance to ensure:

- IT is aligned with the business
- IT enables the business and maximises benefits
- IT resources are used responsibly
- IT risks are managed appropriately

## RISK MITIGATION

WHY EUROSUX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

## CHOOSING THE RIGHT PARTNER

Legislation, standards and frameworks are technology-neutral: vendors, however, are not. A whole range of suppliers, from the world's largest system integrators to established telecommunications operators are competing for the hearts and wallets of pan-European organisations, safe in the knowledge that confusion and fear bring guaranteed revenue streams. This makes due diligence an essential requirement when selecting any kind of partner.

The following questions can help you when sizing up an IT/telecoms partner:

- 1) Can your partner prove it is regularly subjected to an ongoing rolling programme of external audits and when did it last have one?
- 2) Does your partner have a history of certification? Eg ISO 27001?
- 3) Does your partner have experience transitioning from one standard to another to ensure a tighter fit with the ongoing evolution of European regulatory framework and standards?
- 4) Does your partner have experience of dealing with a range of highly regulated industries?

- 5) Can your partner demonstrate an in-depth knowledge of compliance issues?

Information security is an essential building block for IT compliance. You should therefore look for a partner who can provide the following policies:

- A network security segmentation policy provides a framework for defence in depth on the network.
- Technology-based policies to cover such issues as the use of encryption or wireless.
- A system-development security policy to ensure that new systems are designed, developed, tested and deployed in a secure manner.
- Individual policies and standards that cover such subjects as risk analysis, information classification, minimum standards for information protection, incident response, investigations, patch management, and malicious software.
- It is essential that your partner should be able to demonstrate its own rigorous processes and pan-European approach to compliance. With ISO certification and working within an ITIL framework, your technology partner should be able to prove it complies with highly stringent demands covering a wide range of controls in all areas of security.

For further information on finding the right compliance partner

[www.colt.net](http://www.colt.net)

This paper is one of a four-part series of COLT and IDG white papers addressing the most pressing issues facing CIOs of major European organisations. The papers address the following themes: resource optimisation ([url](#)), risk mitigation ([url](#)), flexible working ([url](#)), business efficiency ([url](#)).

## RISK MITIGATION

WHY EUROSUX COMPLIANCE SHOULD BE VIEWED AS A BUSINESS OPPORTUNITY

## CONCLUSION

Effective compliance offers better control of IT assets, as well as the ability to demonstrate compliance to your customers and prospects.

When implemented in tandem with the right partner, it can help you lower the risk of significant costs to business such as lost revenue, productivity, legal penalties and brand damage.

It can improve the integrity of information and provide quick access to the right information for customers, regulatory bodies and legal entities, helping you to mitigate the risk of prosecution and reap financial rewards.

### A roundup of the benefits of compliance

- Reduced operational and business risks
- Enhanced business resilience and performance
- Lower costs due to fewer incidents, reduced downtime, more efficient utilisation of assets
- Revenue protection (preserving access to business functions and avoiding losses associated with negative impacts to reputation and productivity)
- End-to-end visibility of services and help to ensure service quality (better customer service)
- Better data protection and confidential intellectual property
- Increased trust and confidence among the stakeholder community

in association with

