



How To Demonstrate Regulatory Compliance

exaprotect

Simplifying Security Management

November 2006

Executive Summary

Increasingly, organizations throughout Europe are expected to comply (and to **demonstrate this compliance** to auditors and external inspectors), with complex, risk-based corporate governance requirements, and a wide range of information-related regulations. This has significant implications for IT governance.

Demonstrating compliance at the business process and IT application level is a lot simpler than doing so at the operating system and general IT infrastructure level. However, business process and IT application level controls depend on effective security at the operating system and general IT infrastructure level.

ExaProtect helps organizations simplify application, operating system and infrastructure-level collection and analysis of all the data that demonstrates their legal and regulatory compliance.

Legal and Regulatory Background

US and EU-based organizations are subject to an extensive range of information and IT-related regulatory requirements.

These fall into four distinct groups:

- Corporate governance requirements, such as the US Sarbanes Oxley Act of 2002 and the UK's Combined Code on Corporate Governance;
- Financial requirements such as those set out in the UK's Financial Services Authority's Rule Book and associated regulations;
- The Basel 2 requirements;
- Sector-specific requirements such as the Payment Card Industry (PCI) Standard.

Corporate governance regimes

The UK's Combined Code is probably the most evolved corporate governance regime in the EU, and one which companies listed on the UK Stock Exchange must comply. In addition, companies with listings in the US will also have to comply with the Sarbanes Oxley Act of 2002 (SOX). The UK's Combined Code is a principles-based governance regime which requires listed companies to comply with its provisions or to provide an explanation for not doing so. SOX, on the other hand, is a rules-based statutory regime, which requires adherence to its provisions on risk of penalty for both the corporation and its officers.

The UK's Corporate Governance regime explicitly requires boards to *"identify, assess and deal with significant risks in all areas, including in information and communications processes"*

Both regimes require organizations to develop, implement, and maintain an internal control framework that will be suitable for and effective in enabling the board to manage risk (primarily, but not exclusively, financial risk) throughout the enterprise. The Turnbull Guidance, which provides guidance to directors on the risk management aspects of the Combined Code, explicitly requires boards, *"...on an ongoing basis, to identify, assess, and deal with significant risks in all areas, including in information and communications processes"*.

i 'Turnbull Guidance', paragraph 21

US Sarbanes Oxley Act (SOX)

SOX requires US listed companies (and, increasingly, there is a knock-through effect on their major suppliers) to annually assess the effectiveness of their internal controls. It also places a number of other significant governance burdens on executive officers, including the section 409 requirement that companies notify the SEC, “...on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer”.

More importantly, under SOX section 404, management is required to certify the company’s financial reports and both management and an independent accountant are required to certify the organization’s internal controls.

In almost every organization, financial reporting depends on the IT infrastructure, whether it is for the rendering of an invoice, the effective operation of an ERP system, or an integrated, organization-wide management information and control system. Unless appropriate internal controls are built into this infrastructure, management will not be able to make the required certification, and will be directly subject to personal and corporate penalties.

Under the Sarbanes-Oxley Act rules, portions of an inspection report that deal with criticisms of, or potential defects in, the firm’s quality control systems can be made public if the firm does not address those matters to the Public Company Accounting Oversight Board’s satisfaction within 12 months after the report date.

The PCAOBⁱⁱ (Public Company Accounting Oversight Board), was created under SOX to oversee the activity of the auditors of public companies in the United States. Its Auditing Standard No 2, dealing with audit of internal control over financial reporting, identifies general controls as the most important component of the internal control system’s control environment. These general controls are explicitly IT-related, and are required to operate at the network and system levels to ensure that the environment within which financial applications operate is secure.

UK Financial Services Authority (FSA) rule book

The 8,800 pages in the FSA’s current Handbook reflect the fact that it was created by amalgamating the rulebooks of all its predecessor UK financial regulators. Some 29,000 firms are regulated by the FSA, which takes a principles-based approach to regulation. This approach is, “...underpinned by the principle that it is neither possible nor desirable to write a rule to cover every specific situation or need for decision that a regulated firm might encounter. Instead, we focus on the Principles set out in the FSMA...” (Financial Services and Markets Act 2000).

These, the High Level Standards, are set out in the Full Handbook, and include:

- Prin 2.1.2 – “A firm must conduct its business with due skill, care and diligence”, and
- Prin 2.1.3 – “A firm must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems”.

In its chapter on Senior Management Arrangements, the Handbook sets out requirements in respect of processes and systems, including SYSC 3A.7.1: “...A firm should establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third party suppliers, agents and others)”.

ii For more information, see www.pcaobus.org

Encouraging firms to take appropriate steps to control operational risks through development of its IT systems, the Handbook states: ‘...IT systems include the computer systems and infrastructure required for the automation of processes, such as application and operating system software; network infrastructure; and desktop, server, and mainframe hardware. Automation may reduce a firm’s exposure to some ‘people risks’ (including by reducing human errors or controlling access rights to enable segregation of duties), but will increase its dependency on the reliability of its IT systems”ⁱⁱⁱ.

The FSA expects regulated firms to control operational risks through its IT systems, and to take account of the risks in - and its dependency on - its computer systems and network infrastructure.

Basel 2 and MiFID

Basel 2, implemented throughout the EU via the Capital Requirements Directive (CRD), applies to banks, building societies and some investment firms and comes into effect in January 2007. In the UK, BIPRU 6^{iv} contains the FSA’s rules on evidencing an effective operational risk^v management approach. This approach, which must be robust and externally validated, must also integrate with the firm’s overall approach to risk management.

The Markets in Financial Instruments Directive (MiFID), comes into force from November 2007. The FSA, responsible for implementing MiFID as well as the CRD, has still (November 2006) to finalise those modules of the Handbook that will relate to these directives. It does intend, however, to “...create a common platform in SYSC of systems and controls requirements to comply with both the CRD and MiFID”^{vi}. In other words, the control requirements identified earlier will be extended to apply to both these regulations as they come into force.

Sector-specific requirements

EU organizations are also subject to a range of other data-related legislation and standards, ranging from the Data Protection Directive (incorporated into UK legislation as the Data Protection Act 1998) through to the Payment Card Industry Data Security Standard (PCI). PCI was published by Visa and MasterCard in January 2005 and was designed to apply to, “...members, merchants and service providers that store payment card information”^{vii}. PCI contains very specific requirements in terms of information security (all of which have been mapped to ISO/IEC 27001:2005, the international standard specification for Information Security Management Systems) and merchants and service providers must conform.

Common themes

There are significant overlaps between many of these detailed requirements and the outcomes of operational risk management decisions that are made in complying with the FSA Handbook or Corporate Governance requirements. The common theme that emerges is the requirement for organizational internal control frameworks to manage risk effectively throughout the organization. These frameworks must take into account the risks in IT systems,

-
- iii FSA Handbook, SYSC 3A.7.5
 - iv BIPRU is the Banking Prudential Sourcebook issued by the FSA to replace their initial ‘interim’ prudential sourcebooks which set out requirements for the behaviour and activity of regulated firms.
 - v The Basel definition of operational risk is “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.” (Operational Risk, BIS, January 2001)
 - vi CP06/3 Strengthening Capital Standards 2, FSA, February 2006
 - vii PCI Standard

and to ensure the confidentiality, availability and integrity of information. **With the exception of the detailed requirements contained in PCI, regulatory requirements are principle-based, not specific.** Organizations are, in other words, required to assess the risks to their business and to develop an internal control framework appropriate to those risks.

A common, underlying theme across these requirements is that organisations must be able to evidence their decision-making process, and the effectiveness of their control decisions.

Control Requirements

An appropriate internal control framework must take account of the need for monitoring the reliability of IT systems, and for information security.

The FSA requirements in respect of information security are specific. Firms must ensure:

1. Confidentiality: information should be accessible only to persons or systems with appropriate authority, which may require firewalls within a system, as well as entry restrictions;
2. Integrity: safeguarding the accuracy and completeness of information and its processing;
3. Availability and authentication: ensuring that appropriately authorised persons or systems have access to the information when required and that their identity is verified;
4. Non-repudiation and accountability: ensuring that the person or system that processed the information cannot deny their actions^{viii}.

These information security controls are part of what are known as 'general controls.' General controls are defined as "...controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all the applications. The objectives of general controls are to ensure the proper development and implementation of applications, and the integrity of program and data files and of computer operations"^{ix}.

Demonstrating Compliance

ISO 27001 is an externally-auditable standard for information security management systems. It deals explicitly with the general control requirements identified above. **Development, implementation and maintenance of an ISO 27001-certified system would clearly be a logical first step for organizations seeking to demonstrate compliance with those requirements.** Whether or not an organization does choose to follow this route, it will still have to identify an effective way of dealing with a number of issues arising from the complexity of today's business networks and IT infrastructures:

- The volume of data processed through those systems;
- The changing universe of persons authorised to access that data;
- The rapidly evolving, mutating information security threat environment.

viii FSA Handbook, SYSC 3A 7.7

ix Glossary of Audit Terms, www.auditnet.org

ISO 27001 and ISO 17799 encourage the use of the Plan-Do-Check-Act (PDCA^x) cycle in the security management process to maintain continuous improvement in the face of ever-evolving threats.

The changing threat environment is of particular importance for today's businesses. Attacks are increasingly blended ones, in which the techniques of hackers, spammers and virus writers are co-ordinated to breach corporate defences. These attacks might be large scale, or they might be focused on only a small number of targets. Where these attacks depend on internal involvement, they are even harder to defend against. The 2005 FBI Computer Crime Survey reported that:

- 87% of organizations experienced a security incident in 2005;
- Viruses, worms, Trojans and spyware formed a "non-stop barrage";
- While antivirus, antispyware, firewalls and antispyam are almost universal, they did little to stop malicious insiders;
- 44% of attacks were from within the organization;
- 25% of attacks were from both inside and outside the organization.

Neither the threat level, nor the range and sophistication of attacks, is likely to decline any time soon.

Unless organisations choose to disconnect from the Internet and return to the pre-networked period, they will have to take (and regulatory authorities will expect to see them take) a more sophisticated approach to countering attacks.

Issues in Achieving Compliance

The traditional approach to achieving compliance in these areas includes monitoring device access information (and attempted access) at the individual event level (i.e. device and access attempt). Anomalous event information can then be investigated, and unauthorised intrusion attempts identified and countered. There are a number of practical barriers to the effectiveness of such an approach.

Volume and range of technical devices and appliances

Most networks today contain a significant number of devices, including workstations, remote access devices (e.g. PDAs, remote laptops), servers, routers, switches and communications devices that often support more than one operating system, and a wide range of applications (both commercial off-the-shelf packages and applications developed in-house) and services, both internal and external. Organizations that have grown by acquisition often contain networks that differ in detail among themselves. Every single one of these devices is likely to have its own Access Control List to generate a log of information which will include details about accesses. Few organizations, though, have the technical expertise and resource to gather this information – which typically runs to tens of thousands of events per hour – in a way that will enable them to analyse it adequately.

x Also known as the Shewhart cycle or the Deming wheel.

False positives

The first challenge is to differentiate between authorised and unauthorised access attempts. While those access attempts that follow a specific path are relatively easy to identify, every incorrect entry of a user name and/or password could appear to be an unauthorised access attempt, even if it was only the result of user error, memory failure, or device error. Each of these errors ('false positives') must be eliminated before the possible attacks can be identified and, by the time they are, it may be too late to counter the attack.

Volume of data unlinked to specific controls

In analysing the range of data, the specific control to which the data relates is not usually clear. For instance, an authorised user seeking access to an unauthorised application might be evidence of an attempted insider attack, or it might be evidence of a delay in amending user access rights. A different response is usually called for in each case, but unless there is some immediate information available as to the nature of control violation, it is difficult for a security administrator to identify an appropriate response.

Data can speak to more than one control requirement

Similarly, an attempted security breach might be evidence of violation of more than one control, each of which will need to be addressed in order to eliminate loopholes. An individual application attack, carried out by someone authorised to access the IT system, is likely to be an 'authorised use' violation; it might also be violation of a 'time-of-day' control, and of a 'segregation of duties' breach. Uncertainty about which control has been breached (and therefore what counter-action to take) can inhibit the security response.

Scenario complexity

Traditional approaches usually fail to identify today's complex and increasingly sophisticated attacks. Individual events, which on their own might be innocuous, might also, when linked together with other events (i.e. correlated), identify a serious control breakdown. For instance, an authorised user accessing the system is unlikely to be identified as an attack. An attempt to transmit information through email is also unlikely to be identified as a security event. However, if the user who had logged in had also recently resigned, was logging in outside of normal hours, and was transmitting information (including client databases) to a Hotmail account, then it would be obvious that a security breach was occurring.

In-house programming and monitoring expertise

Traditionally, organizations who attempt to monitor individual events, (at a level of granularity that will enable them to arrive at better quality decisions about many of these scenarios) rely on third party software whose configuration and operation depends on their developing, in-house, significant programming, and monitoring expertise. This is expensive and is not an option open to all organizations; it also gives rise to its own set of control challenges in terms of ensuring the effectiveness of the software.

What Might the Ideal Solution Look Like?

Ideally, an organization's Chief Security Officer would have a software product that continually monitors all activity (human and device) across the network, compares events to the organization's own security policy and controls, and which gives a report that says, in effect, 'Everything's green, apart from x, y & z'. In considering solutions that might deliver such an outcome, there are a number of key criteria that should be considered.

Critically, any solution must deal with more than just perimeter security. While it is important to gather and analyse perimeter security events (at firewalls, VPN servers, etc), ***it is more important to monitor events throughout the network, and particularly at the network's core, where corporate information and intellectual property is created, modified, accessed or stored.*** Inclusion of this core security monitoring with the traditional peripheral security monitoring means that any solution must be capable of managing a very high level of events, and to track user and device activity at all stages of any session.

Experience shows that a typical correlation of events to alerts is in the order of 1000:1; that is, one alert for every thousand events. This means that an ideal solution must:

- Provide end-to-end session tracking, that supports both real-time security event monitoring, and subsequent security audits;
- Have very fast real-time correlation, processing (depending on the size of the network) between 5,000 and 15,000 events per second;
- Authenticate and encrypt events that are transmitted;
- Provide graphical reports to a central office which identify high risk alerts and that go back to the original initiation date of the system;
- Have sufficient online storage for at least three months of events;
- Be capable of easily adding new event sources (whether new applications, new devices, or new occurrences of existing devices);
- Be capable of easy updating for new scenarios and emerging threats;
- Support segregation of administrative duties;
- Have a high availability option, and a tested disaster recovery capability.

Of course, any solution today also needs to be easy to deploy and manage; analyst and system administrator training should require no more than, say, one to two days, and it should not be necessary to develop and maintain an expensive internal skill bank to support the security solution.

Most important of all, a solution must integrate into the organisation's existing or planned security management processes and procedures.

How Does ExaProtect Deliver an Ideal Solution?

ExaProtect meets all these criteria, and supports the requirements of ISO 27001.

ExaProtect's Security Management Solution monitors critical business assets, behaviours and sessions, collecting events of all types from all the peripheral and core devices across the network, and can process in excess of 15,000 events per seconds. Events are stored in a database, where they are standardized and enriched to enable correlation and comparison of different events on different devices.



Events, and sequences of events, are then automatically compared to pre-determined scenarios (a scenario contains a sequence of events linked to a specific control implementation that will evidence compliance or non-compliance with a pre-determined corporate policy) and those that should be flagged are reported in real-time in a dashboard style console.

Ease of configuration is an essential ExaProtect characteristic. New threats and security threats are constantly emerging; speed and flexibility in creating new scenarios, against which they can be assessed, is built into ExaProtect's Security Management Solution.

Finally, a comprehensive suite of auditable reports is available to demonstrate to external auditors and to regulators that the organization has taken – and continues to take – appropriate and effective steps to monitor and manage in real-time all the risks to their information and IT systems.



Simplifying Security Management

ExaProtect is a unique global player in the information security marketplace, offering a complete start-to-finish security management solution. Our powerful integrated 'View & Do' approach is of great benefit to our 300+ existing customers, who include many Fortune 500 enterprises, international telecommunications companies and government organizations.

Our technology empowers you to meet the increasing demand for unified control of multi-vendor network and security systems, whether your goal is to raise information security levels, demonstrate compliance, and/or improve operational efficiency.

Our US headquarters is based out of Mountain View, California, and our EMEA headquarters is based out of Paris, France. With 7 offices worldwide, we deliver a global solution.

For more information and local contact details, please visit: www.exaprotect.com

Contact ExaProtect for more information or to arrange a demonstration:

US Headquarters:
Mountain View, CA
Phone : +1 650 428 2800
Email: info@exaprotect.com

EMEA HQ, Sales France and Southern Europe:
Paris, France
Phone : +33 (0)1 47 15 04 00
Email: info@exaprotect.com

Sales UK, Northern Europe and South Africa:
Cambridge, UK
Phone: +44 (0)8450 549 900
Email: info@exaprotect.com

Sales Germany and Central Europe:
Düsseldorf, Germany
Phone : +49 (0)211 52 391 550
Email: info@exaprotect.com

Technical Services Centre:
Lyon, France
Phone : +33 (0)4 26 23 25 25
Email: info@exaprotect.com
