DeviceLock for Compliance with the Combined Code on Corporate Governance (UK)

Contents

Introduction

The corporate governance systems of public companies listed on the London Stock Exchange (LSE) are governed by the Combined Code on Corporate Governance. The principles, rules and requirements set out in the Combined Code are aimed at increasing the effectiveness of information disclosure, thus increasing the transparency of public companies. They are also meant to put into place the means for internal control over financial reports and corporate assets in order to protect shareholder interests.

Unlike the United State's very strict Sarbanes-Oxley Act of 2002 (SOX), the Combined Code's requirements are not mandatory. However, if the management of a public company refuses to implement the rules or principles of the Code, it must provide a clear argument to investors defending its position. More often than not, the easiest route for a company is to follow best practices as they are set out in the Code, rather than to ignore them.

At the same time, the Combined Code does have quite a bit in common with SOX, in particular, SOX's well-known Clause 404. This clause requires that a company put an internal control system into place. Some guiding principles for this were set out in the Turnbull Report of 1999.

According to this report, public companies in the UK should create an internal control system aimed at counteracting fraud and protecting corporate assets against theft, appropriation and other abuses. In practice this means that a corporation must introduce control procedures for reports and assets. These days, financial reports are compiled in electronic format, and a company's most important assets include intellectual property, confidential information and client databases. In other words, internal control must be built on information technologies in order to track operations with assets and reports.

This document will describe the requirements of the Combined Code. These requirements influence the information infrastructure of an organization and the means of security that are used within that infrastructure. This document will also introduce DeviceLock, a product from DeviceLock, Inc., which can be used by organizations to considerably improve compliance with the Combined Code on Corporate Governance.

Combined Code Requirements

The Combined Code is comprised of several sections; each section is a report named after the person who oversaw the preparation of the report.

The first Combined Code was comprised of the Cadbury, Greenbury, and Hampel Reports and came into force on January 1, 1999. Later, the Code was supplemented with the Turnbull, Myners, Smith, Higgs and Tyson Reports.

In the end, the Financial Reporting Council brought together all of the Reports and released a new revision of the Combined Code in July 2003, which came into effect on 1 November 2003.

Table 1 below lists the most important reports which make up the body of the modern system of corporate governance in Great Britain.

Corporate Governance in Great Britain		
Name	Publication Date	Explanation
The Cadbury Report	**December 1992**	Financial aspects of corporate governance
The Rutteman Report	**December 1994**	Internal control and financial reporting
The Greenbury Report	**July 1995**	Remuneration for members of the board of directors
The Hampel Report	**January 1998**	Fundamental principles of corporate governance
The Combined Code	**June 1998**	Principles of good governance and a code of advanced experience
The Turnbull Report	**September 1999**	An internal control system
The Myners Report	**March 2001**	Institutional investors
The Smith Report	**January 2003**	The audit committee under the board of directors
The Higgs Report	**January 2003**	The rule of non-executive directors
The Tyson Report	**June 2003**	Hiring and training non-executive directors
The Combined Code	**July 2003**	The Combined Code of Corporate Governance

Table 1. Corporate governance standards in Great Britain.

How is the Combined Code Different from SOX?

The main difference between SOX and the Combined Code is that the British corporate governance system is not strictly regulated. It functions under the rules of “comply or explain.” This means that all corporations with stock listed on the London Stock Exchange must annually publish year-end reports comprised of two parts. The first section discloses how the company applies the principles of the Combined Code. The second section must either confirm compliance with the regulations and provisions of the Combined Code, or explain the reasons why the company has deviated from any of the requirements.

As a result, market players voluntarily accept or reject the Code's provisions. British experts believe that this approach recommends itself well, and that it will not require revisions now or in the near future. Furthermore, the new latest version of the Combined Code (from 2003) only emphasizes the voluntary nature of the Code. The principles of corporate governance have been divided into key principles, and auxiliary principles. As a result, companies have even greater flexibility in taking decisions.

The Code does not govern the format of year-end reports. In other words, a corporation's management team must decide independently which provisions of the Combined Code to address in the report, how to prove the effective implementation of Code principles, and how to explain deviations from Code guidelines.

The Key Components of the Combined Code

In addition to the key requirements, one third of the 2003 version of the Combined Code is comprised of three explanatory documents: the Turnbull Report on creating an internal control system, the Smith Report on the functions of the audit committee, and the Higgs Report on ensuring effective corporate governance.

It is important to note that the Turnbull Report (on creating an internal control system) replaced the Rutteman Report on internal control and financial reporting, which was featured in the first version of the Code. Later, in October 2005, the Turnbull Report was also replaced by a different document released by the Financial Reporting Council. The new document is called: Internal Control – Revised Guidance for Directors on the Combined Code. This Report has been in effect since January 1, 2006.

The Internal Control System under the Combined Code

According to Principle C.2 of the Combined Code: "*The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets*." Further, Code Provision C.2.1 reads: "*The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so*." This review, according to the Code, must include control over the material, financial and organizational bases of the corporation, as well as the risk management system (including statutory risks).

Creating an internal control system is directly related to its subsequent audit. As Provision C.3.1 requires that the board of directors form an audit committee. The functions of the audit committee are set out in Provision C.3.2 and include: monitoring the integrity of the financial statements of the company, reviewing the company's internal financial controls, and reviewing the company's internal control and risk management systems.

The Turnbull Report (2005) provides an explanation of what is meant by "a *sound system of internal control*." According to Paragraphs No. 15 and No. 16, it first and foremost means a system which minimizes all potential risks regarded as unacceptable for the company to bear. In other words, minimizing risks which can be avoided or minimized.

Let us consider Paragraph No. 19: "*An internal control system encompasses the policies, processes, tasks, behaviors and other aspects of a company that, taken together: facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud…*" etc. Within a sound internal control system, responsibilities must be clearly delegated for different classes of corporate assets.

According to Paragraph No. 19, the system must *help ensure the quality of internal and external reporting and help ensure compliance with applicable laws and regulations*. In addition to functions which are meant to ensure compliance, an internal control system can also help to boost a company's competitiveness.

Features of "a *sound internal control system*" include the following:

- monitoring processes (Para No. 20);
- *procedures for reporting immediately to appropriate levels of management any significant control failings or weaknesses* (Para No. 21);
- *protection with certainty against a company failing to meet its business objectives or all material errors, losses, fraud, or breaches of laws or regulations* (Para No. 23).

At the same time, Paragraph No. 26 addresses issues concerning the audit of internal control mechanisms and indicates that key components of a "sound" system of internal control include continuous monitoring and the ability to produce regular reports on the state of internal control resources.

DeviceLock from DeviceLock, Inc.

DeviceLock is endpoint device control software developed by DeviceLock, Inc. (formerly SmartLine Inc) for corporate users. With DeviceLock, a company of any size can ensure comprehensive control over data which leaves a corporate network via the ports, wireless networks, external drives, and printers attached or integrated into a Microsoft Windows workstation endpoint. In contrast to the great number of solutions that sift through email correspondence to detect leakage of sensitive data, DeviceLock gives security administrators the power to judiciously shut user access to workstation ports and drives so that data leakage doesn't happen in the first place. Should security administrators choose to leave endpoint resources unlocked, DeviceLock provides for the collection and analysis of data leaving the corporate network via workstation ports and drives including documents sent to local and network printers. In other words, DeviceLock not only controls access to endpoint input/output resources based on assigned policies, it can also "shadow" all outgoing data so that audit and forensic experts have the evidence they need to prove compliance or catch malfeasance.

There is an ever-increasing number of mobile devices maintained and, in some cases, purchased by employees connecting to corporate networks. Experts at Yankee Group and SCS Research studied this trend toward the '*consumerization of corporate IT networks*' and advised IT department managers and directors neither to ignore nor to attempt to completely prohibit the plethora of portable devices used by employees. They simply must provide support for employees' mobile computers. Otherwise, the company risks losing its innovative and competitive edges by reducing the productivity of its employees. Meanwhile, mass consumerism is rife with new, serious risks in information security, as mobile devices may be used for fraudulent purposes, information leaks and other internal breaches. DeviceLock can help solve that problem.

When it comes to PDAs, smartphones and other communicators, DeviceLock does more than just support the shadow copying of all of the data exchanged to a Windows Mobile® or Palm® OS personal mobile device - it also allows a company to apply flexible security policies and then track the enforcement of these policies. For example, DeviceLock may permit a user to synchronize his contacts and calendar, but prohibit copying files or synchronizing email with attachments.

DeviceLock also provides protection against hardware keyloggers, which are connected between a computer's keyboard and the system unit and used to steal valuable data from employee workstations. A malicious user can connect a keylogger between an employee's computer and keyboard, thus tricking antivirus software and other means of security. Once DeviceLock detects the exchange of data from the computer to the keylogger, it will block the keylogger, warn the user and create a record in the events log.

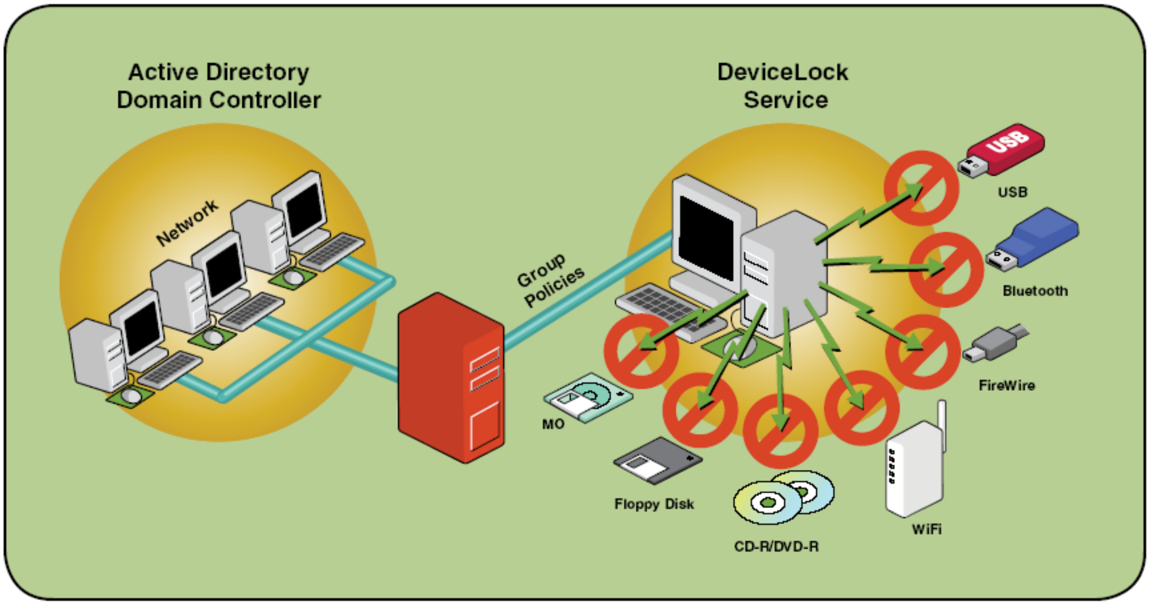
Through all these features, DeviceLock protects companies against the leakage of consumer information and unwanted content, and serves as a tool for retrospective analysis of all data which company employees copy to external drives or personal mobile devices and take with them, as well as send to local, network and even virtual printers. It also affords a company the flexibility it needs to set up information security policies for mobile devices.

DeviceLock consists of three parts: the agent, the server and the management console:

1. DeviceLock Service (the agent) is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.

2. DeviceLock Enterprise Server (the server) is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data.

3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor).



DeviceLock can be controlled using group policies in Windows Active Directory, making it easy to integrate it into the infrastructure of an organization of any size.

How DeviceLock Can Help Create an Internal Control System

DeviceLock helps to control the exchange of data via local workstation ports, wireless networks and removable drives based on flexible policies. It automatically makes the decision to either permit or prohibit access to a removable device based on a high-precision permissions strategy set by an authorized security administrator. DeviceLock's settings and policies are easily audited, and DeviceLock itself does not create any additional information security risks.

Using DeviceLock in a corporate environment helps ensure compliance with the key provisions of the Combined Code on Corporate Governance, in accordance with Principle C.2. In this context, DeviceLock is a necessary component of the internal control system, which can facilitate the management of access rights to local ports and interfaces and different types of data synchronization. Using DeviceLock effectively will considerably minimize the risk of uncontrolled leakage of intellectual property and confidential documents, which can have a significant positive effect for company shareholders.

The table below (Table 2) summarizes the features of DeviceLock and how they help support compliance with the Combined Code on Corporate Governance.

DeviceLock and Compliance with the Combined Code	
Combined Code Requirements	DeviceLock Features
Principle C.2: the board of directors must maintain a sound system of internal control in order to protect shareholder investments and corporate assets	DeviceLock provides one element of an internal control system by controlling the exchange of data leaving workstations via their local ports or wireless networks. In addition, DeviceLock makes it possible to apply flexible security policies when working with PDAs, smartphones and communicators by permitting some operations and prohibiting others. This means DeviceLock reduces the risk of uncontrolled leakage of confidential information and the theft of intellectual property and the data assets of a company.
Provision C.2.1: the board of directors must review the effectiveness of the internal control system	Thanks to DeviceLock, a company's management team has one less thing to worry about: in line with this provision, DeviceLock's automatic mode can help to control the exchange of data, including a company's information assets, via workstation ports, wireless networks, removable drives, and printers. At the same time, DeviceLock's settings and policies are fully auditable. In addition to shadow copying, DeviceLock also compiles an events log which records all of the data exchange operations executed by a user between the workstation computer and an external medium via ports and wireless networks, as well as local or network printers. This is an important feature, as this kind of log is mandatory for conducting successful audits of corporate information systems.
Provision C.3.2: the board of directors must ensure that the following functions are carried out: monitoring the integrity of financial reports, reviewing control over financial reports, reviewing the internal control system and the risk management system	Shadow copying data that leaves the corporate network via workstation ports, removable drives, personal mobile devices, printers and wireless networks is a feature unique to DeviceLock. DeviceLock stores all outgoing data in an external Microsoft SQL Server database, which facilitates subsequent audits, retrospective analyses and investigations into the leakage or theft of data assets.

About DeviceLock, Inc.

DeviceLock, Inc. (formerly SmartLine Inc) was established in 1996 to provide effective and economical network management solutions to small, medium and large-scale business. Early on, we made it our mission to design software that is robust and reliable when it comes to enforcing network policy, while being easy and intuitive for system administrators to use. Furthermore, we made it our job to deliver solutions that are well-integrated and cost-effective. Based on this formula, we've introduced and developed category-leading products like DeviceLock for enforcing security policy related to personal devices.

DeviceLock, Inc. is a worldwide leader in endpoint device control security. Our DeviceLock product is currently installed on more than 3 million computers in more than 55 000 organizations around the world.

The company's customers include BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, and various state and federal government agencies and departments.

DeviceLock, Inc. is an international organization with offices in San Ramon (California), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).

Contact Information

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germany

TEL: +49 (2102) 89211-0
FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milan, Italy

TEL: +39-02-86391432
FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, UK

TEL (toll-free): +44-(0)-800-047-0969
FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA

TEL (toll-free): +1-866-668-5625
FAX: +1-646-349-2996

sales@devicelock.com

support@devicelock.com

www.devicelock.com