DeviceLock for Basel II Compliance

Contents

Introduction

Basel II (full name: The International Convergence of Capital Measurement and Capital Standards: A Revised Framework[1]), is the second of the Basel Accords and poses minimum capital requirements. In line with the framework, financial companies must assess their operational, market and credit risks and form capital reserves to cover these risks.

A portion of these requirements, which deal specifically with credit and market risks, were already addressed in the first Basel Accord. That is why one of the key new requirements of Basel II means that banks must also manage operational risks, which include IT threats and the malicious actions of employees.

The more effectively a bank manages an operational risk, the less capital it is required to reserve for that risk. As a result, a bank will be left with more available funds, which in turn has a positive impact on the bank's competitiveness.

This document will analyze the requirements of Basel II in terms of operational risks, the structure of these risks and their influence on a company's information infrastructure. Moreover, this paper will address the opportunities afforded by DeviceLock, Inc.'s product DeviceLock, which can help banks minimize the operational risks that pose a threat to information security.

Basel II Requirements

According to Clause 644 of Basel II: "*Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk*."

It is clear that this definition of operational risks encompasses primarily information security threats resulting from employee interaction with a bank's information systems. For example, the malicious actions of insiders (such as the theft of confidential information, fraud, negligence and inconsistency) are included in the concept of operational risk and may cause a bank to incur significant damages. Those committing violations from the inside may steal confidential company reports or private client data.

According to the definition of operational risks in Clause 644, reputational risk falls into a different category. Consequently, these risks do not impact the requirements for capital adequacy. Nevertheless, according to the third point[2] of the first principle of the supervisory process[3] and Clause 732, "all material risks faced by the bank should be addressed in the capital assessment

[1] Full English document: http://www.bis.org/publ/bcbs128.pdf
[2] "Comprehensive Risk Assessment"
[3] The first principle is: "Banks should have a process for assessing their overall capital adequacy in relation to their risk profile and a strategy for maintaining their capital levels."

process." Clause 742 stipulates that material risks must absolutely include reputational risks. Although the Basel Committee admits that this type of risk is not easy to measure, it still recommends developing reputational risk management methods. That means that banks are expected to do everything in their power in order to ensure maximum risk management, including for reputational risks.

The connection between operational and reputational risk is important. For example, the manifestation of many insider threats which are directly related to operational risk (according to Clause 644) can also lead to other negative consequences in the form of a sullied image and damaged reputation. This concept is confirmed by the latest study by Deloitte[4]. If there is a leak of confidential information, or if insiders steal from the bank's clients, etc., the public at large may well find out about it. As a result, the company's image is tarnished, which leads to a decline in the client base and reduced profits. In other works, reputational risks may be the direct result of existent operational risks.

Essentially, the Basel II Accord requires that a bank manage its operational risks, which by definition include information security threats in general and insider risks in particular. Moreover, the document recommends that banks engage in reputational risk management, and reputational risks can often result from the exhibition of internal information security threats.

Assessing Operational Risks

Clause 645 of the Basel II Accord sets out three approaches for calculating operational risk capital requirements based on a spectrum of increasing sophistication and risk sensitivity: (i) the Basic Indicator Approach (ii) the Standardized Approach and (iii) Advanced Measurement Approaches (AMA). It is presumed that banks will move along this chain of approaches as they develop more advanced operational risk management systems and practices.

The simplest method is the **Base Indicator Approach**, covered in more detail in Clause 649. Banks using the Basic Indicator Approach must hold capital for operational risk equal to the average over the previous three years of a fixed percentage of positive annual gross income. Figures for any year in which annual gross income is negative or zero should be excluded from both the numerator and denominator when calculating the average.

Clause 660 outlines the **Standardized Approach**, under which a bank must prove to regulatory bodies that it satisfies three key criteria. First, a bank's board of directors and senior management must be actively and appropriately involved in the oversight of the operational risk management framework. Second, the bank must have an operational risk management system that is conceptually sound and which is implemented with integrity. Finally, the third criterion is ensuring that the bank has sufficient resources in the use of the approach in major business lines[5] as well as in the control and audit areas.

The formal requirements of the **Advanced Measurement Approaches** (AMA) are in part the same as the conditions listed above, but differ in that there are somewhat stricter requirements for the operational risk management system (Clause 664). The bank must also have an independent department (function) responsible for developing and laying in an operational risk management mechanism. In addition, the bank's internal operational risk assessment system must be closely integrated with current risk management processes within the bank, and the results are to constitute an integral part of the operational risk structural monitoring and control

[4] For more information, see the report issued by Deloitte and Ponemon Institute: "Enterprise@Risk: 2007 Privacy & Data Protection Survey."
http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf

[5] The principles for categorizing the bank's operations by business lines are addressed in Appendix 6 of the Basel II Accord.

processes. For example, that information must play a key role in compiling risk reports, management reports, as well as the internal allocation of capital and risk analysis.

Using AMA also presumes regular risk reports and reporting division-level losses to management, senior management and the board of directors. In other words, the bank must track potential and existent operational risks and ensure that there is an opportunity to assess any damages.

Furthermore, the bank must have procedures for taking measures based on information contained in management reports. Consequently, the bank's operational risk management system must be well documented, and the bank itself must also have a compliance mechanism for documenting internal strategies, control procedures and operational risk management, including measures to be taken in the event of noncompliance.

The Basel Committee assigns a key role to internal and external auditors, who must regularly audit management processes and the operational risk assessment system. Operations at various levels are also audited for operational risk management, including business units and separate departments.

The more complex the operational risk management system applied by a bank under Basel II, the more precisely it will be able to assess potential losses resulting from a specific risk; risks will be better managed, and losses will be avoided. In other words, it is in a bank's best interests to follow these approaches and gradually move towards more advanced operational risk assessment systems and practices.

DeviceLock from DeviceLock, Inc.

DeviceLock is endpoint device security software developed by DeviceLock, Inc. primarily in order to minimize internal information security risks. DeviceLock also helps companies achieve compliance with even the most complex requirements and regulations.

With DeviceLock, a company of any size can protect itself from the theft, leakage and corruption of information secured on corporate networks. DeviceLock controls all uploading and downloading activity via workstation ports, wireless networks and external drives based on assigned policies. When configured for the purpose, it can also provide complete shadow copying of all outgoing data. 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 computers. As a result, DeviceLock minimizes the most dangerous kinds of operational risks.

When data shadowing is activated, DeviceLock registers all required data for audit purposes in compliance with Basel II, and keeps records of incidents resulting from existing information security threats. Meanwhile, this function also provides the bank with an information base for assessing losses and identifying reasons behind the emergence of a risk.

DeviceLock is highly flexible when it comes to working with mobile devices (PDAs, smartphones, and other types of communicators). DeviceLock does more than support shadow copying of all of the data exchanged to a 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 protects companies against leakage of digital assets and unwanted content and serves as a tool for retrospective analysis of all data which company employees copy to external drives and take with them. DeviceLock also provides companies with the flexibility they need when working with mobile devices.

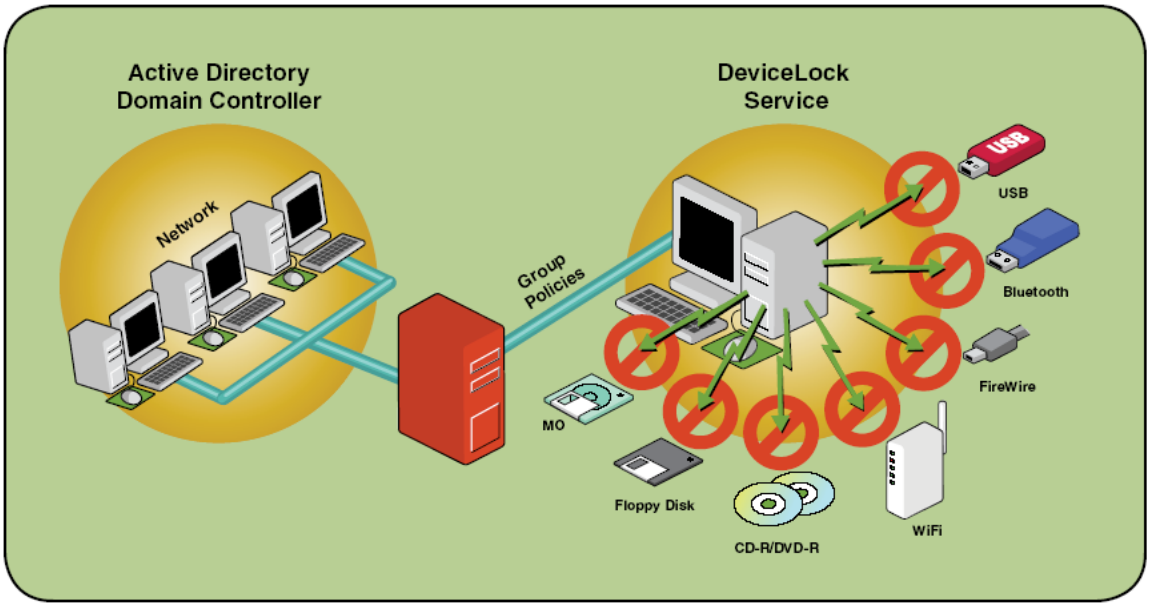
DeviceLock can be used to control a full range of potential points of data leakage: USB ports, disk drives, CD and DVD drives, FireWire, IR ports, parallel and serial ports, WiFi and Bluetooth adapters, tape recordings, PDAs, any internal and external removable drives and hard drives. DeviceLock conducts a thorough audit of user actions with these devices and data.

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 Supports Basel II Compliance

DeviceLock controls data movement via local workstation ports, wireless networks and removable drives based on flexible policies. Each time, the decision to either permit or prohibit access to an external device is made automatically. That means DeviceLock does not create any additional operational risks within the bank, and that all operations to configure and adjust DeviceLock's settings are fully recorded and can be used in subsequent audits, which is a very important feature in terms of Basel II compliance.

In summary, using DeviceLock in a corporate environment helps ensure compliance with the two key provisions of Basel II:

- **DeviceLock helps companies take control of internal information security threats, many of which represent operational risks.** As discussed above, the actions of insiders aimed at the theft of confidential or private information are classified as operational risks. The manifestation of these threats can lead to reputational risks, which can damage a company even further. DeviceLock can help a company take control over the data exchange process, and the points at which users interact with the information system via local personal computers, thus effectively counteracting data leakage and minimizing a key component of operational risk.

- **DeviceLock helps collect and analyze data leaving the corporate network via workstations.** By using DeviceLock's shadow copying feature, a bank can easily track the movement of confidential information as well as personal and financial data if they leave the network on a removable drive, a mobile device or via a wireless network. That means the bank can track potential operational risks, and if necessary, assess any resulting damages. These data are the key to compiling risk reports and reporting losses, which are important functions that must be discharged in order to achieve Basel II compliance.

The table below (Table 1) summarizes the features of DeviceLock and how they facilitate compliance with Basel II.

Table 1. How DeviceLock Features Support Basel II Compliance

Basel II Provisions	DeviceLock Features
§40. The calculation of total minimum capital requirements [is made based on] credit, market and operational risks.	Previously, banks managed only credit and market risks, but these days they need to ensure control over operational risks as well. DeviceLock minimizes the most dangerous kinds of operational risks: information security risks. By using DeviceLock, a bank can minimize the risk of the leakage of personal and financial data, confidential information, and can protect corporate networks from unwanted content.
§644. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.	By definition, information security threats constitute a major component of operational risks. Furthermore, Basel II focuses on internal threats resulting from accidental or intentional actions on the part of employees. DeviceLock can help banks in this kind of situation. Data leakage risks are fully under control with DeviceLock, and the bank will be able to insure itself against additional reputational risks which often result from the leakage of clients' private data.
§645. [Basel II] presents three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity: (i) the Basic Indicator Approach (ii) the Standardized Approach and (iii) Advanced Measurement Approaches (AMA).	The more complex a risk assessment method is, the more precise it will be, and that means more money saved for the bank. DeviceLock minimizes some operational risks and creates a mechanism for the audit and tracking of risk exposures, for example, the leakage of confidential data. This feature also creates an information base for the company necessary for compiling reports on operational risks and losses, which is a mandatory requirement for more advanced assessment methods.

§666. A bank must meet the following qualitative standards before it is permitted to use an AMA for operational risk capital: There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports.	DeviceLock's shadow copying feature lets companies save copies of all of the data that leaves the corporate network. It also serves as a tool to determine who copied data, and when and where that data was copied from a workstation. That information is sufficient in order to assess the damage from an operational risk exposure - and that is a major part of meeting Basel II compliance for banks that wish to make the transition to effective operational risk assessment methods.
§732. All material risks faced by the bank should be addressed in the capital assessment process. This includes reputational risks in line with §742.	DeviceLock helps minimize a bank's reputational risks, the nature of which depends heavily on operation risks. DeviceLock allows banks to minimize the most dangerous type of operational threat: the leakage of confidential information. Moreover, it is the theft, unauthorized disclosure and leakage of sensitive data which are frequently the sources of the most dangerous reputational risks which can, in some cases, cause a company to border on bankruptcy.

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