

The role of IT in fulfilling legal, regulatory and industry requirements (compliance)



## GFS/TQS Compliance with the Requirements of the New Basel Capital Accord (Basel II)



## Introduction

In the past few years we have witnessed a wide range of laws, standards and industry regulations being adopted, such as the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standard, Gramm-Leachy Bliley Act, SB 1386 and Basel II.

Each one of these regulations has specific context, implications and goals but, in general, their main purpose is to establish rules that ensure the adoption of good practices of corporate governance and transparency in market relations.

It is common sense that all these regulations have a direct impact, to a lesser or greater extent, on the how companies process and store information. Paradoxically, however, it is difficult to find organizations that can clearly define how their systems environment should be modified in order to comply with the requirements of the regulations that directly affect them.

The difficulty stems mainly from the fact that regulations are made for general-purpose applications. Therefore, regulations only establish minimum criteria on how business should be conducted and they do not provide specific recommendations on how to handle information. For example, regulations state that confidentiality of information should be ensured, but they do not specify how this should be done or what tools should be used. In fact, companies themselves, knowing the specific features of their environments, should create the IT solutions required to fulfill their business requirements.

Similarly, as a systems solutions company, the role of GFS Software is to show its clients how the applications developed by GFS can help them make their environments compliant with the requirements of various regulations.

Particularly, GFS/TQS – Tape Quality System is an application that was conceived and especially designed to help companies fulfill compliance requirements. The purpose of this series of documents is to show how TQS addresses the requirements of each law, standard or regulation.

This document specifically addresses the requirements of the New Basel Capital Accord (Basel II).

## The New Basel Capital Accord (Basel II)

Basel accords are banking supervision agreements (recommendations for drawing up bills), namely Basel I and Basel II, established by the Basel Committee on Banking Supervision (Basel is the name of the city in Switzerland where this committee holds its meetings).

### *The Basel Committee*

It is composed of representatives of central banks, supervisory authorities and regulatory agencies of the finance industry from G10 countries, Luxemburg and Spain. The committee has no authority to demand the implementation of the recommendations, although most member countries and even non-member countries tend to implement the committee policies. This means that these recommendations become requirements through the creation of national laws in each country.

## ***The Basel Accord***

Broadly speaking, the Basel accord addresses risk management in banking institutions. Its goal is to establish rules that minimize risks and protect banks from bankruptcy and, should it occur, to make sure that banks retain enough capital to cover for unexpected losses.

Here are the risks in the banking industry:

- Credit risk
- Country risk and transfer risk
- Market risk
- Interest rate risk
- Liquidity risk
- Operational risk
- Legal risk
- Reputation risk

## **Risks that can be minimized by IT efforts**

Operational, legal and reputation risks can be managed or minimized with the support of IT resources.

### **Operational Risk**

The most relevant types of operational risk involve the collapse of internal controls and corporate domain. Such collapses can lead to financial losses caused by errors, frauds or failure to perform the required activities on a timely basis. In addition, they may otherwise adversely affect bank interests, for example, by means of their dealers, credit granting agents and other administrative components, as a result of overreaching use of their powers or competences or by conducting business in a risky or unethical manner. Other types of operational risk include severe deficiencies in information technology systems or incidents such as major fire or other types of disaster.

### **Legal Risk**

Banks are subject to several types of legal risk. This category includes the risk of having unexpectedly high levels of asset devaluation or liabilities valuation due to legal documents or reports that are inappropriate or incorrect. In addition, the existing legislation can fail in resolving legal issues that involve a bank. A law suit involving a bank can have far-reaching implications to the entire banking industry and can result in costs, not only to the organization directly involved in the law suit, but also to many other banks or all of them. Besides, there may be changes in the legislation that affect banks or other business enterprises. Banks are particularly susceptible to legal risks when they adopt new types of transactions and when the legal right of a counterpart in a transaction is not defined. In addition, in a law suit, severe penalties can be imposed should documents and information not be provided within the established deadlines.

### **Reputation risk**

Reputation risks are related, among other causes, to operational failures and failure to comply with relevant laws and regulations. Reputation risks are particularly harmful to banks, since the nature of their business requires depositors, creditors and the market in general to trust in banks.

## Compliance of IT resources with Basel II requirements

IT resources are compliant with the requirements of the New Basel Capital Accord whenever they help to reduce risks or when they provide control and supervisory tasks required to properly manage risks.

Specifically, one application helps fulfilling the Basel II requirements if it implements one or more processes / systems that can:

1. Prevent the inappropriate disclosure of information
2. Prevent unauthorized transactions
3. Prevent unauthorized changes in systems (when those systems are developed or managed) that allow fraudulent transactions to be conducted; to loosen control and monitoring of certain operations or disable audit logs (in order to allow certain actions to go unnoticed).
4. Prevent transactions from being intercepted and changed when information is transferred through communication channels.
5. Prevent service interruption caused by hardware or software failures.

These features can be implemented using IT resources that aim at ensuring the following aspects in information processing, transmission and storage:

- Confidentiality
- Integrity
- Availability
- Audit trails and logs
- Authentication / authenticity

## How GFS/TQS reduces risks

GFS/TQS was specifically designed to help companies meet their compliance requirements of information storage in magnetic tapes, thus minimizing or eliminating some types of risk.

GFS/TQS reduces risks by implementing features and functions to:

1. Prevent service interruption caused by hardware or software failures – thus reducing the probability of media failure and ensuring more availability of critical information to operations or to fulfill legal requirements;
2. Prevent unauthorized transactions – using authenticity certification, which clearly indicates the occurrence of fraud in files, thus making this practice much more difficult.

Through its functions and features, GFS/TQS positively affect the following aspects involved in information processing, transmission and storage:

- Protection of file **integrity**
- Increased **availability** of information
- Assurance of **authenticity** of the file content (evidence of non-tampering)

## ***Reduction of operational risks***

Through the use of GFS/TQS and by observing the conditions that it establishes, GFS/TQS ensures that old tapes that are improper for use can be immediately identified and replaced. Therefore, all other tapes being used in an organization will be suitable to store information reliably.

By ensuring that only quality tapes are maintained and through operations of certification of reading (which periodically show the availability of critical information), GFS/TQS minimizes the possibility of losing critical data to the operational processes due to failures in magnetic media.

Therefore, GFS/TQS ensures not only the integrity of information but also its availability, thus reducing downtime losses in production or losses caused by the need of reprocessing.

Concurrently, GFS/TQS implements an important feature to control errors and frauds: the certification of authenticity, which can show that stored files have not been subject to any type of modification, whether accidentally or intentionally, thus reducing the risk of fraud.

## ***Reduction of legal risks***

Today a significant amount of information needs maintain its integrity and availability during periods that are much longer than the specified durability of media, even in the case of modern media types. It is not rare to see cases where information needs to be stored for 4 or 5 decades, while the most modern tapes last 15 to 20 years approximately.

The unavailability of information may subject the company to fines or other penalties, which may even include the arrest of its legal representatives (for example, failure to submit information that is required by court orders, within the established deadlines).

GFS/TQS automatically identifies media that have reached the end of their shelf life and transfers data from them to new media, thus ensuring the availability of information that needs to be stored for long periods of time due to legal requirements.

In addition, the unique functionality of certification of authenticity provided by GFS/TQS can prove to authorities and auditors the authenticity of the required files.

GFS/TQS also maintains a complete database related to the files that are stored on tape. The product includes a wide range of reports that can show the risk control efforts being made, which meets important audit requirements.

## ***Reduction of reputation risks***

By reducing the risks of operational failures and failure to fully comply with relevant laws and regulations, GFS/TQS ultimately reduces the risks related to reputation damage.

## Bibliography

BASEL COMMITTEE ON BANKING SUPERVISION. **Core Principles for Effective Banking Supervision**. Translated by Jorge R. Carneiro. Brasília: Brazil Central Bank, 1997. Available at: <<http://www.bcb.gov.br/ftp/defis/basileia.pdf>>. Accessed on Dec 21, 2006.

SECURITY INNOVATION, INC. **Regulatory Compliance Demystified: An Introduction to Compliance for Developers**. [S.l]: Microsoft, 2006. Available at: <[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/regcompliance\\_demystified.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/regcompliance_demystified.asp)>. Accessed on Dec 21, 2006.