*Ana Savić**

DOI: 10.2298/EKA0876088S

# MANAGING IT-RELATED OPERATIONAL RISKS

**ABSTRACT:** *Not so long ago, information technology (IT) risk occupied a small corner of operational risk – the opportunity loss from a missed IT development deadline. Today, the success of an entire financial institution may lay on managing a broad landscape of IT risks. IT risk is a potential damage to an organisation's value, resulting from inadequate managing of processes and technologies. IT risk includes the failure to respond to security and privacy requirements, as well as many other issues such as: human error, internal fraud through software manipulation, external fraud by intruders, obsolesce in applications and machines, reliability issues or mismanagement. The World Economic Forum provides best information about this problem. They rank a breakdown of critical information infrastructure among the most likely core global risks, with 10-20 % likelihood over the next 10 years and potential worldwide impact of $250 billion. Sustained investment in IT – almost $1.2 trillion or 29% of 2006 private-sector capital investment in the U.S. alone fuels growing exposure to IT risk. Greg Hughes, chief strategy officer in Symantec Corp. recently claimed "IT risk management is more than using technology to solve security problems. With proper planning and broad support, it can give an organization the confidence to innovate, using IT to outdistance competitors".*

**KEY WORDS:** *information technology risk, operational risk, security, system reliability*

**JEL CLASSIFICATION:** G20, O30.

* ICT College, Belgrade

## 1. Introduction

Accidents, environmental disasters, bankruptcy, and loss of business are risks that have plagued the human race since their early days. Unfortunately, there is no complete protection against every risk, but there are some measures that can be taken to reduce potential losses. Risk management has started its development since 1980s, and nowadays it is a very important part of financial company's general management. By monitoring risk more closely, financial organisations can minimise the required amount of reserve capital and maximise their profitability.

Just recently, financial organisations have started focusing on operational risk. Before that, they were focusing on developing sophisticated tools for measuring market and credit risk. The main characteristic of operational risk is that unlike market and credit risks, which mainly involve risks associated with trading or lending, everyone in the financial organisation can be a source of operational risk. Although operational risk is not a new risk, globalization of financial services, growing sophistication of financial technologies and new business activities, are making operational risk profile more complex (level of operational risk probability, exposure and impact throughout all organisation's activities).

The fact is that of all different types of risks that can occur in financial organisation, operational risks can be among the most destructive and most difficult to foresee. One highly visible operational risk event can suddenly end the life of a financial organisation. For that reason, regulators are examining these risks under several acts: the Bank Secrecy Act, USA Patriot Act, Gramm-Leach-Billey Act, Basel II Accord, Sarbanes-Oxley, and Federal Financial Institutions Examination Council (FFIEC) guidelines.

The Bank Secrecy Act and the USA Patriot Act require programs to be in place for anti-money-laundering, reporting of suspicious activity, large cash transactions, customer identification and more. The Gramm-Leach-Billey Act requires safeguards for customer information, privacy, and information security. The Serbanes-Oxley Act requires internal control reviews across most departments, which are a subset of the bank wide risk assessment process.

The FFIEC and FFIEC IT handbooks direct senior management and the board of directors to manage IT risks, including information security, business continuity and disaster recovery.

In addition, of course, there is the Basel II Accord, which focuses on bringing together the world's financial organisations under a common regulatory framework. Basel's main focus is on creating regulation guidelines on the "standardization of risk management" for financial organisations. These standards, aiming for a closer correspondence between the capital that banks hold and the risks they take, should lead to more stable and efficiently run financial organisations.

Anyway, operational risks are present whether the business is regulated or deregulated, centralized or decentralized, old technology or high technology, locally based or international... Though it tends to increase with sophistication of financial instruments, and as business characteristics vary operational risks tend to change. Therefore, to a large extent, each financial institution has its own profile of operational risks.

## 2. Defining operational risk

The term "operational risk" has been defined only in the past few years, although this type of risk has been present for years. At first, it was commonly defined as "every type of non-quantifiable risk faced by a bank", or "everything other than credit and market risk"… Nowadays, there is a large number of definitions, but the most appropriate is the one given by the Basel Committee on Banking Supervision: "operational risk is the risk of losses resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk[1], but excludes strategic and reputational risks[2]". Of course, under new regulatory rules, each bank will be allowed to adopt its own definition of operational risk.

If we put it very simply, we can say that operational risk is the risk associated with everyday activities of an organisation, which involves the management of the performance of its processes, its people, and its systems, to reach the expected business performance. Operational risks include breakdowns in internal controls and corporate governance, which can lead to financial losses through frauds, or failure to carry out operations in timely manner. Other aspects of operational

1 Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements. Basel Committee on Banking Supervision (June 2006), *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, http://www.bis.org/bcbs/publ.htm, p.144

2 Almost all banks rejected the idea of including strategic and business risk in a regulatory capital charge, although many allocate economic capital for this.

risks include major failure of IT systems, or even events such as major fires or other disasters…

Operational risk can be very clearly presented through five major operational risk categories:

1. organisation
2. processes and policies
3. systems and technology
4. people
5. external events

One of the main characteristics of operational risks is that those categories are related to a certain degree, and are partially overlapping (e.g. people, systems and technology in a financial organisation interact to produce a successful process - or unsuccessful one).

There are some main factors which represent the drivers for operational risks at a present time: new products, product sophistication, new distribution channels, new markets, new technology, complexity of technology, e-commerce, business volume, new legislation, globalization, regulatory pressure, mergers and acquisitions, reorganisations, staff turnover, cultural diversity of staff and clients.

In years to come, financial organisations will face two major drivers that will challenge them to take on additional and partly new operational risks: globalization and Internet-related technologies. The reason for this is the fact that no part of banking has changed as significantly during the past ten years as the area of information technologies (IT), and we can only imagine what it will bring us in years to come.

## 3. Information technology risk (IT risk)

In an advanced industrial society, a company's operations are highly dependent on the integrity of its technology systems. Its success depends, in a great part, on its ability to use increasingly rich databases, and make timely decisions connected to industry changes. A financial organisation's performance is negatively impacted if it experiences system interruptions, errors, or even if it falls behind its competitors concerning the information technology, which it

uses, and in what way it is using it. So, every organisation has to be committed to an ongoing process of upgrading, enhancing and testing its technology, so it can effectively meet: sophisticated client requirements, market and regulatory changes and internal needs for information management.

Information technology risk includes the failure to respond to these requirements, as well as many other issues such as: human error, internal fraud through software manipulation, external fraud by intruders, obsolesce in applications and machines, reliability issues, mismanagement, and of course the effect of natural disasters. This risk is definitely manageable, but it takes a significant amount of skill to do it, and maybe the most important thing is that a strong team is needed, constituted both of economic and engineering experts.

Information Technology (IT) systems have become critical to every aspect of business, resulting in a fact that IT risk, once a minor component of operational risk, is emerging as a major hazard for organisations to identify and manage. IT risk includes security, availability, performance and compliance elements, each with its own origins.

Generally speaking, IT risk is a potential damage to an organisation's value, resulting from inadequate managing of processes and technologies. From the technology point of view, the main risks are: breaches in established defenses, poor configuration without risk analysis, sabotage of data or systems, malicious software, updating antivirus and antispyware programs, access to confidential data, unauthorised access by unauthorised personnel, technology made to monitor and manage system performance…

As mentioned before, not so long ago, IT risk occupied a small corner of operational risk – the opportunity loss from a missed IT development deadline. Today, the success of entire organisation may hinge on managing a broad landscape of IT risks. The World Economic Forum provides best information about this problem. They rank a breakdown of critical information infrastructure among the most likely core global risks, with 10 to 20 percent likelihood over the next 10 years and potential worldwide impact of $250 billion[3]. Sustained investment in IT – almost $1.2 trillion or 29% of 2006 private-sector capital investment in the U.S. alone fuels growing exposure to IT risk.

3 World Economic Forum, *Global Risks 2007: a Global Risk Network Report* (Geneva, January 2007), http://www.weforum.org/pdf/CSI/Global_Risks_2007.pdf, p.8

According to Sydneylink Pty Ltd data (based on the answers of 639 examinees) the total loss in 2005, which was the consequence of computer crime and bad security measures, was 130,104,542 $. According to that questionnaire, the loss was caused in the first place by attacks connected with viruses, followed by steeling of information and forbidden access. These three categories are elements of IT risks, and could be prevented with taking adequate measures and with good risk management. The interesting information gathered in the same questionnaire was that 96% of examinees had been using anti virus programs, 97% of them had had firewall, and 25% had bought specially secured technologies. Such enormously high level of implementation of security measures compared with such big losses indicates either inadequate implementation of software or hardware, or unskilful use of them, which is definitely a problem of managing IT risks.

One of the Worlds' most famous corporations for security and software making - Symantec, is building solutions daily to help individuals and enterprises assure the security, availability, and integrity of their information. Their key findings made in their IT Risk Management Report Volume 1 (published in 2007), which was the result of a year-long study that examined IT risk based on interviews with more than 500 IT executives and professionals around the world, are that organisations in year 2006 anticipated major information loss and compliance failures at surprisingly high frequencies:

66 % expect a major regulatory incident at least once every 5 years
58 % expect a major data loss at least once every 5 years
60 % expect a major IT incident at least once a year.

Furthermore, connected with the previously given definition of IT risk as "a potential damage to an organisation's value, resulting from inadequate managing of processes and technologies", they found out that organisations are more effective in implementing technology controls than process controls - shortcomings are in areas that can have a negative impact in overall IT Risk Management. In this research, they set levels to classify organisations as Strong, Good, Weak and Poor, at implementing and deploying technology controls or process controls. This can be seen in Figure 1.

**Figure 1**. IT Risk Management Process vs. Technology Effectiveness[4] (Effectiveness Index)

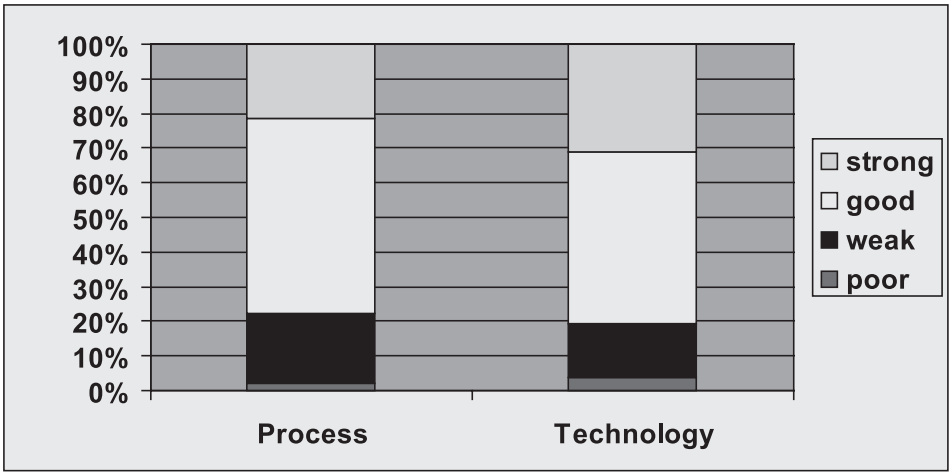



Figure 1 compares these effectiveness ratings, and it shows that organisations are generally more effective implementing technology than process: 33% rated Strong on the technology effectiveness index, and only 25% rated Strong on the process effectiveness index[5]. Of course, the most effective IT Risk Management Programs use well-defined controls that combine well-chosen technologies and best-practice processes. Furthermore, they discovered that best-in-class organisations perceive higher risk levels, but experience fewer IT incidents. Those organisations were more effective in implementing the entire range of controls.

Over the years, available computer power has enormously increased, which is not followed in the same amount by applications and system solutions. This dissonance between spending money on information technology and getting tangible benefits of it is again problem of the management.

Financial organisations always benefit from advanced, highly competitive computer applications, but those organisations that are slow in implementing high technologies or perform poor quality applications will definitely have bad results. Figure 2 shows this bifurcation.

4 ent-it_risk_management_report_02-2007.en-us.pdf, www.symantec.com, p.18

5 These indexes average ratings for eight individual factors concerning process or technology controls.

**Figure 2**. Available computer power applied through advanced or lagging IT applications[6]

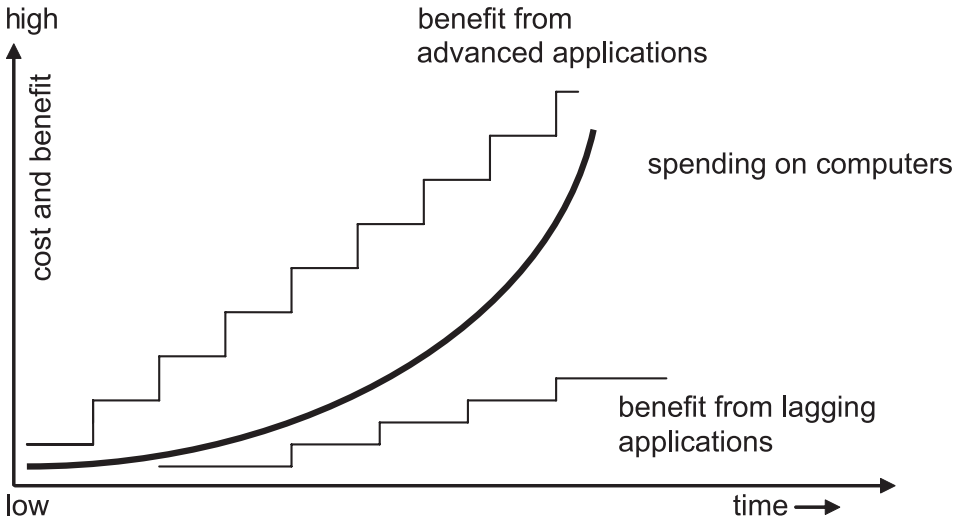



Figure 2 draws attention to the fact that while practically all companies nowadays spend large amounts of money on computers, communications and software, only the leaders really benefit from their investments. Spending big sums of money on technology without the corresponding return on investment (ROI) is an IT-related operational risk, and is closely connected to the management process in organisations.

Electronic banking was made possible because of technology. By doing banking activities electronically, the complexity of business operations increased significantly, and it was even more intensified by the ongoing process of concentration in the banking industry. However, while mergers and acquisitions are often seen as a means for cost savings, ROI is very rarely a clear goal concerning approving IT costs.

IT is an integral part of many business operations and transactions, and furthermore, virtually the entire business may be carried out across IT systems and networks, always being aware that IT risk evolves as fast as technology changes.

6 Chorafas D (2005), *Operational Risk control with Basel II – Basic Principles and Capital Requirements*, Elsevier finance, Oxford, p.92.

For example, online "phishing" fraud (with legal and regulatory requirements for IT countermeasures) was virtually unknown just three years ago.

## 4. Classifying IT risk

Identification, analysis, measurement and management of IT risk, requires specialized knowledge and skill. IT risk management has to be done in every organisation, and every organisation has its own unique IT risk profile. IT risks can be classified according to their impact on the organisation[7], as follows:

1. security risk
2. availability risk
3. performance risk
4. compliance risk

*Security risk* – the information will be altered, accessed, or used by unauthorised parties. Sources of security risk could be: external attacks, malicious code, physical destruction, inappropriate access, unsatisfied employees, variety of platform and messaging types.

Potential impacts associated with them are: corruption of information, external fraud, identity theft, theft of financial assets, damage to reputation and damage to assets.

Availability risk – that information or applications will be inaccessible due to system failure or natural disaster, including any recovery period. Sources of availability risk are: hardware failures, network outages, data centre failures, force majeure.

Potential impacts associated with them are: abandoned transactions and lost sales, reduced customer, partner, or employee confidence, interruption or delay of business critical processes, reduced IT staff productivity…

Performance risk – that underperformance of systems, applications, or personnel, or IT as a whole will diminish business productivity or value. Sources of performance risk are: poor system architectures, network congestion, inefficient code, inadequate capacity.

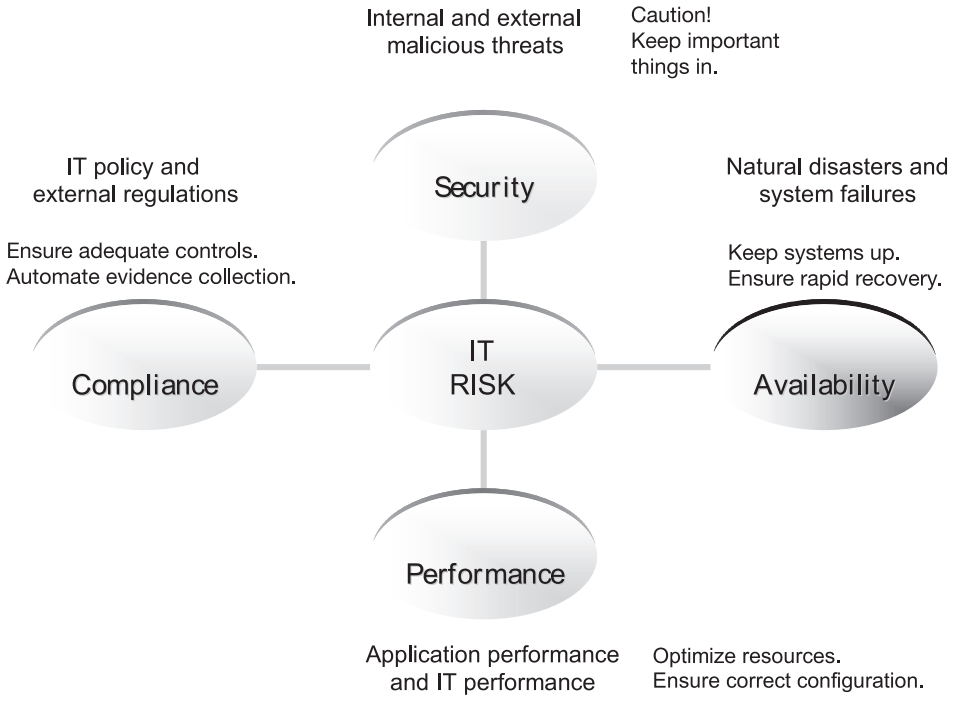
7 ent-it_risk_management_report_02-2007.en-us.pdf, www.symantec.com, p.7

Potential impacts associated with them are: reduced client satisfaction and loyalty, interruption or delay of business critical process, lost IT productivity…

Compliance risk – that information handling or processing will fail to meet regulatory, IT or business policy requirements. Usually, it involves penalties, fines, or loss of reputation from failure to comply with laws or regulations, or consequences of non-compliance with IT policies. Sources of compliance risk are: regulations unique to each jurisdiction (including Graham-Leach-Bliley act, EU Data Protection Directive, Sarbanes-Oxley act…), legal actions, internal IT safeguards supporting compliance, inadequate third-party compliance standards. Potential impacts associated with them are: damage to reputation, breach of client confidentiality, litigation…

These four areas of IT risk are shown in Figure 3, each with its own set of drivers and potential impacts.

**Figure 3**. IT risks spanning in four areas



## 5. System reliability as a major objective

*Reliability* in a company is the probability that a given component or system (or subsystem) will perform without failure over a pre-established period of time and under conditions which characterize the operations this component or system is expected to perform[8]. System reliability or the lack of system reliability is a major operational risk, and one of the strong IT risks.

Reliability of a given system component is often confused with reliability of a whole system, and this is completely wrong. The main rule is that the more complex the system is, the faster its reliability decreases. There is a possibility of making a relationship between system reliability (R) and component reliability (r). The algorithm connecting this two is:

$$R = e^{-t / \check{T}} \tag{1}$$

where:

e= the radix of Neperian (natural) logarithm
t= the pre-established operational period
Ť= Mean time between failures (MTBF)

MTFB is basic metrics in engineering.

Another key measurement is mean time to repair (MTTR). With information system, we are also interested in other metrics:

- MTBSI which stands for mean time between systems interrupts
- MTOSI which means mean time of system interrupt

Reliability may also be defined as the extent to which a system or component performs its specified functions without any failures visible to the user. In this broader sense, instead of the reliability equation (1) many computer centres prefer to use the following calculation:

$$R = \frac{\text{System usage time}}{\text{Sum of interruptions}} \tag{2}$$

8 Chorafas, D (2005), *Operational Risk control with Basel II – Basic Principles and Capital Requirements*, Elsevier finance, Oxford, p.105

The total system facilities viewed as an integral source of a given technological capability can be categorized according to the responsibility of the provider of IT services, and according to the job done by the end-user of those facilities. Hardware, software, communications, and operational reasons will all have an impact on systems availability.

*Availability* is the probability that a system is running at any point during scheduled time[9]. It is calculated as follows:

$$\text{Percentage availability} = 100 \text{ x } \frac{\text{System usage time (uptime)}}{\text{Scheduled time}} \qquad (3)$$

where Uptime = Scheduled time – System downtime

Availability and reliability relate to the system running at any point during scheduled time. They also define the extent to which the system (all components of hardware, software, and documentation provided by the supplier) may be dependent upon to provide complete, correct results when requested, given any combination of inputs. Some inputs can be invalid, not because of unreliability of the system, but because of other reasons. Complete and correct results require error detection, correction and publication.

Furthermore, reliability, availability and business continuity correlate. Operational risk must be examined from the viewpoint of all possible consequences to an entity, because it can suffer a disaster that can stop it functioning properly (e.g. total system failure or some wider disruption can be caused by several reasons, including power outages – which is not hardware or software failure).

In addition, reasons for system outages sometimes involve problems with vendor-supplied trading system software, which is perfect example of lack of coordination in outsourcing. A lot of companies operating on-line rely on vendor support for major parts of order processing. When these third-party systems experience problems, outages hit more than only one firm. This leads us to the next point that operational risk may result from IT outsourcing.

9 Chorafas, D (2005), *Operational Risk control with Basel II – Basic Principles and Capital Requirements*, Elsevier finance, Oxford, p.107

## 6. Operational risk that may result from IT outsourcing

New developing banking practices in recent years brought new and growing risks to banks. One source of risk is definitely growing use of outsourcing arrangements. *Outsourcing* is the delegation to another party (the *insourcer*[10]) of the authority for providing the services. Basel Committee on Banking Supervision defines outsourcing as a "regulated entity's use of a third party…to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future"[11]. There are different types of outsourcer-insourcer relations, but outsourcing is always done under a contract that incorporates service level agreements, including functionality, cost, quality and timeliness of deliverables. The insourcer, who is the third party, accepts the rendering of specific services, under the mentioned four conditions.

Companies outsourcing their information technology, or other services, must understand that risks and responsibilities cannot be delegated by the outsourcer to the insourcer. They stay in the responsibility of the board and CEO. Of course, every insourcer is faced with the challenge of getting the job right, or the cost of getting it wrong. So, having this in mind, it is obvious that there are risks associated both with outsourcing as well as insourcing.

The first step is making decision whether to outsource or not. The main rule, concerning this question is: never outsource (or insource) what you don't understand. Moving away from this principle is the same as assuming a mass of operational risks. Operational risk associated to outsourced services must be properly identified and controlled *before* the contract is signed.

Companies give different reasons for outsourcing services. Most frequent reasons are: reduction of costs, focus on core business, improve functional performance or quality, improve time to market and foster innovation. Of course, we have to be aware that not all these reasons are always true (e.g. costs are not necessarily reduced through outsourcing).

There is an example of an investment bank which outsourced its IT to downsize its employment by transferring its own IT personnel to the insourcer, and these

10 Chorafas D (2003), *Outsourcing, Insourcing and IT for Enterprise Management*, Macmillan/ Palgrave, London.

11 Basel Committee on Banking Supervision (February 2005), The Joint Forum, *Outsourcing in Financial Services*, BIS, , http://www.bis.org/bcbs/publ.htm, p.4

personnel continued to work on the bank's premises[12]. The services provided by its former personnel were billed by the insourcer to the bank at a higher rate, with the result that the overall expense instead of being downsized went up.

The question whether outsourcing is a good policy cannot be answered in a general sense. But there is one important general rule, and that is that core functions should not be outsourced, or should be outsourced with exaggerated attention.

IT outsourcing can be considered as extremely important and delicate. Moreover, regulators have not been particularly happy with the practice of IT outsourcing, because while it may diminish some operational risks, it brings out other operational risks. For that reason, Federal Deposit Insurance Corporation (FDIC) gives some guidelines on choosing a software/service bureau outsourcer for banks:

- Information technology is core business in banking
- Failure in outsourcing can be as fatal to a financial institution as failure of its own IT resources
- The board, CEO, and senior management have personal accountability for all outsourced service.

The Outsourcing Institute has conducted surveys of various companies and organisations on their outsourcing practices, and according to their 5th Annual Outsourcing Index, activities being outsourced include the following[13]: Transportation (9%), Real Estate/Facilities Management (11%), Sales/Marketing (13%), Contact Centres/Call Centres (15%), Manufacturing (18%), Human Resources (19%), Finance (20%), Distribution and Logistics (22%), Administration (47%) and Information Technology (55%). This survey shows that IT related services appear to be the most frequently outsourced activities.

The Federal Financial Institutions Examination Council (FFIEC) published Information Technology Examination Handbook "Outsourcing Technology Services Booklet" in June 2004, which provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage and monitor IT outsourcing relationships. Financial institutions can outsource many areas of operations,

12 Chorafas D (2003), *Outsourcing, Insourcing and IT for Enterprise Management*, Macmillan/Palgrave, London.

13 Basel Committee on Banking Supervision (February 2005), The Joint Forum, *Outsourcing in Financial Services*, BIS, , http://www.bis.org/bcbs/publ.htm, p.5

including all or just part of any service, process or system operation. Examples of IT operations frequently outsourced by institutions (which are also subject of this booklet) are: the origination, processing and settlement of payments and financial transactions, information processing related to customer account creation and maintenance, as well as other information and transaction processing activities that support critical banking functions, such as loan processing, deposit processing, trading activities, security monitoring and testing, system development and maintenance, network operations, help desk operations and call centres. Financial institution has the responsibility to manage the risks associated with these outsourced IT services. So the ultimate decision whether to outsource should fit into the institution's overall strategic plan and corporate objectives.

They have to be aware that outsourcing does not reduce the fundamental risks associated with information technology or the business lines that use it. Risks such as loss of funds, loss of competitive advantage or damaged reputation remain. Because the functions are preformed by an organisation outside the financial institution, the risks may be realized in a different manner than if the functions were inside the institution, definitely resulting in the need for controls designed to monitor every aspect of such risks.

Banking and information technology are indivisible. Technology is a financial institution's infrastructure, and no bank can function with defective IT regardless of whether it is provided in-house or it is outsourced.

## 7. IT trends through 2007

As the world grows more dependent on IT systems and processes, management of IT risk becomes a necessity. IT risk encompasses the full spectrum of risks that may effect or result from IT operations: external natural disasters or changes in government regulation, internal processes that effect product or service quality, IT organisational and data centre performance, loss of intellectual property, supervisory or legal controls, and much more.

In a modern world, every organisation has its own unique IT risk profile. It is connected to the fact that we are witnesses of transition from a hacker culture of nuisance virus outbreaks and network vandalism to an underground criminal economy in which bank accounts, compromised servers, passwords and credit cards are bought and sold in bulk. Professionalization and commercialization of malicious activities, along with more intense attacks and more frequent outages,

have raised awareness and regulatory attention across the entire spectrum of IT risks.

Symantec Corporation published its IT Risk Management Report Volume 2 in January 2008, which follows IT trends through December 2007[14]. They collected 405 surveys from IT professionals attending IT events worldwide during 2007. They found out that nowadays we are facing some new emerging issues with important implications for IT risk management, especially:

- data leakage – risks to an organisation's information assets from both external malicious activity and internal errors
- endpoint management – the need to extend policy-based control over fixed and mobile endpoints in sprawling, porous, worldwide networks
- data centre virtualization – IT risk management implications of adopting virtualization technologies to improve utilization and productivity of storage and services
- zero-day exploits – the need for new defences as the time needed to create and disseminate malicious code that exploits a published vulnerability converges on zero.

Security risk was mentioned above as an undeniably important risk. External attacks, malicious code released onto public networks (with ever-shrinking latency), and attempts of unauthorised access to information and systems remain significant burdens for IT departments worldwide. An alarming development of professionalization of computer crime was documented, especially in industries with high-volume or high-value electronic transactions. This risk compromise customer trust, and customers expect and demand that organisations protect their personal information and money. Customers are especially hard on companies they see as careless with their information – a 2007 consumer survey on data security showed 62% of consumers were more upset when information loss is due to negligence rather than theft. The scale of these breaches is also known – the average incident exposes the personal information of 785000 customers[15]. The 2007 loss by the UK government of more than 7 million families' financial records underscores the risk[16].

14 b-it_risk_management_report_2_01-2008_12818026.en-us.pdf, www.symantec.com

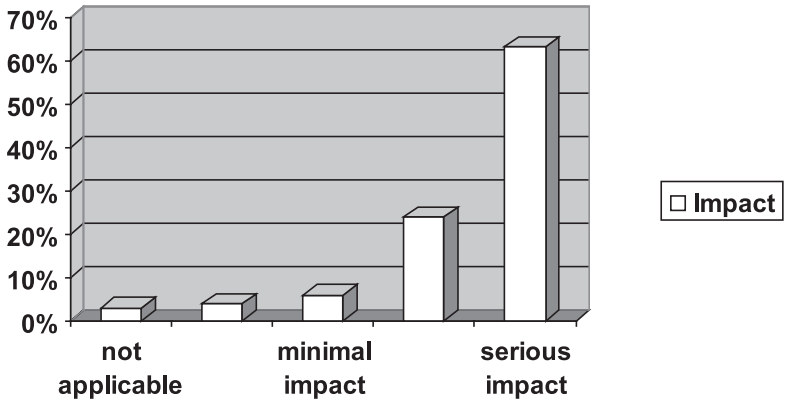
15 Info watch, *Global Data Leakage Survey 2006*, Moscow, February 15,2007, www.infowatch.com/threats?chapter=162971949&id=207784626

16 http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm

Customers withdraw from transaction providers they do not trust, so the data leakage constitutes a serious threat not only to consumers, but to electronic commerce and banking too. In the U.S., financial losses from credit card are assigned to issuers, insulating cardholders from direct financial risk. But new forms of fraud (phishing, pharming, identity theft, underground marketing of private information) threaten reputation, creditworthiness, privacy, autonomy, and other non-financial assets. Of course, the same conditions apply in electronic banking, securities and currency trading, where IT security risks present a direct threat to the liquidity of financial markets.

Symantec Corporation's IT Risk Management Report Volume 2 shows that IT professionals agree with their customers about the gravity of data leakage (as only one of the IT risks): 63% believe a data leak would have serious impact on their business (shown in Figure 4).

**Figure 4.** Data leakage – Impact on business[17]

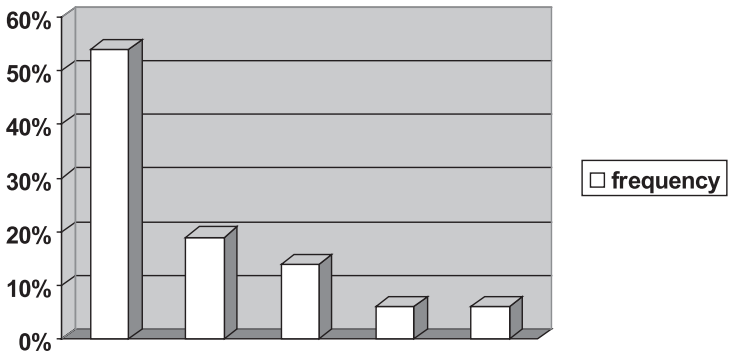



However, despite seriousness of impacts data leakage can make, most of the participants during year 2007 judged that the probability of major data leakage incident at their organisation is quite small: only 19% of them expect incidents as often as once a year. Majority of them - 54% expects incidents only once every five years (Figure 5). The main question is if this is a realistic assessment or if the participants are underestimating this risk? Or are they maybe overestimating the effectiveness of their mitigation strategies?

17 b-it_risk_management_report_2_01-2008_12818026.en-us.pdf, www.symantec.com, p.12

Maybe the explanation of this problem lies in the fact that calculation of incident rates for data leakage is very complicated due to: lack of consistency in reporting standards across organisations and jurisdictions; an understandable reluctance of victimized organisations to disclose incidents except to their customers and as required by law; twofold "threshold" problem: smaller incidents may not be widely reported so incident rates seem lower but average impacts seem higher; and a misguided focus on criminal activity, although most breaches are due to employee error. Because of these factors, data leakage incident information may be reported in fragmented style, leading to lower predictions of incident frequency.

**Figure 5**. Estimated frequency of data leakage (expected incident rate)[18]




Although IT professionals agree with consumers about the severity of data leakage incidents, they definitely underestimate their frequency.

Nowadays, there is a broad availability of stolen data ready for sale on the Internet. Identities, complete with US bank account, credit card, government-issued identification numbers and birthdates, are available for purchase on-line from US $14 to $18.

A lot of people connected with financial organisations primarily identify IT risks as security risks. Probably the word "risk" is more easily applied to security than to performance, availability or compliance. Anyway, overestimating security risk can cause misallocation of time and resources, and significant exposure to other IT risks. Even when security risk becomes the most important one in the organisation, which was the case in some organisations during the year 2007, it

18 b-it_risk_management_report_2_01-2008_12818026.en-us.pdf, www.symantec.com, p.13

has to be considered in balance with the full range of IT risk elements. For every type of IT risk, there is a compromised core value, as follows:

- Security risk – trust, customer reputation
- Compliance risk – legal, financial and operational integrity
- Performance risk – efficiency and productivity
- Availability risk – financial and supply-chain integrity, commercial responsibility

Compliance risk, for example, is often seen as derivative of "security", since many regulations govern privacy and information security. But compliance risk is more than just security risk formalized by law. The US Sarbanes-Oxley Act of 2002 and the EU Markets in Financial Instruments Directive are two recent examples of regulatory initiatives not aimed at security risk, but with strong consequences for IT. The compliance obligations are subject to local, regional and national regulations, and they include the costs of maintaining and reporting compliance to the satisfaction of external regulators, the challenges of setting and meeting internal policies and standards to assure that external requirements are met, and obligations governing the security, availability and performance of their IT services for internal clients.

## 8. Conclusion

As the world grows more dependent on IT systems and processes, management of IT risk becomes a necessity. IT risk (encompassing security, availability, performance and compliance elements) has become a critical issue for executives and board of directors.

It is considered to be a part of Operational risk, which encompasses processes to address events coming from fraud or fire to supply-chain failure. Diversity of operational risk events is captured in its definition: "the risk of losses resulting from inadequate or failed internal processes, people and systems, or from external events", covering risks that cannot be completely hedged or insured against.

IT risk alone, encompasses the full spectrum of risks that may effect or result from IT operations: external natural disasters or changes in governmental regulation, internal processes that effect product or service quality, IT organisational and data centre performance, loss of intellectual property, supervisory or legal

controls and much more. The main classification of IT risks is done according to their source and potential impact on financial institutions, and it includes:

- Security risk – that information will be accessed, manipulated or used by unauthorised party,
- Availability risk – that information or applications will be made inaccessible by process, people or systems failures, or natural disasters,
- Performance risk – that underperforming systems, applications, staff, or organisations will diminish business productivity or value,
- Compliance risk – that information handling or processing will fail to meet regulatory, IT or business policy requirements.

Financial institution's assets, operations and staff may be brought to harm by internal or external threats carried out or weaknesses exposed across IT networks and systems.

Managing IT risks is extremely important part of Financial Risk Management, and it helps keeping IT services flexible, adaptive and aligned to financial institution's goals in a constantly changing environment (managing IT risk definitely doesn't mean eliminating it). IT risk management has to understand completely IT risks, and to explore not only negative impacts on institution's performances, but how these risks can make contribution to business productivity, competitive advantage and the spirit of innovation.

IT risk management can provide the insight that allows financial institution to take calculated risks with confidence and use IT to drive competitive advantage. Greg Hughes, chief strategy officer in Symantec Corporation, the global leader in infrastructure software, recently claimed: "IT risk management is more than using technology to solve security problems. With proper planning and broad support it can give an organisation the confidence to innovate, using IT to outdistance competitors".

## REFERENCES

Basel Committee on Banking Supervision (Feb. 2003), "Sound Practices for the Management and Supervision of Opertional Risk", http://www.bis.org/publ/bcbs86.htm

Basel Committee on Banking Supervision (February 2005), The Joint Forum, "Outsourcing in Financial Services", BIS, http://www.bis.org/bcbs/publ.htm

Basel Committee on Banking Supervision (July 2003), "Risk Management Principles for Electronic Banking", http://www.bis.org/publ/bcbs98.pdf

Basel Committee on Banking Supervision (June 2006), "International Convergence of Capital Measurement and Capital Standards: A Revised Framework", http://www.bis.org/bcbs/publ.htm

BBC news (20 November 2007), "UK's families put on fraud alert", http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm

CERIAS (Centre for Education and Research in Information Assurance and Security): www.cerias.purdue.edu

Chorafas, D (2003), Outsourcing, Insourcing and IT for Enterprise Management, Maacmillan/Palgrave, London

Chorafas, D (2005), Operational Risk control with Basel II – Basic Principles and Capital Requirements, Elsevier finance, Oxford.

CIS (Centre for Internet Security): www.cisecurity.org

Computer Security Resource Centre: www.csrc.nist.gov

CSI (Computer Security Institute): www.gocsi.com

Federal Deposit Insurance Corporation, http://www.fdic.gov

Federal Financial Institutions Examination Council's (FFIEC) http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf

Info Watch (2007), *Global Data Leakage Survey 2006*, Moscow, February 15 2007, www.infowatch.com/threats?chapter=162971949&id=207784626

Information about common criteria for international standards (ISO 17799) connected with testing system efficiency and security, www.commoncriteria.org

*IT Risk Management* (2007), Trends through December 2006, Volume 1, www.symantec.com

*IT Risk Management* (2008), Trends through December 2007, Volume 2, www.symantec.com

Jordan, E and Silcock, L (2005), Beating IT Risks, John Wiley & Sons Ltd. England

Kaiser, T and Kohne, M (2006), An Introduction to Operational Risk, Risk books, Great Britain

McCarthy, L (2003), IT Security: Risking the Corporation, Prentice Hall, USA

World Economic Forum (January 2007), "Global Risks 2007: a Global Risk Network Report", Geneva, http://www.weforum.org/pdf/CSI/Global_Risks_2007.pdf