# IS/IT RISK MANAGEMENT IN BANKING INDUSTRY

**Vlasta Svatá, Martin Fleischmann***

## 1. Introduction

Headlines related to the financial crisis highlighted that significant risk failures persist despite the investments in the risk assessment and risk management disciplines. While isolated incidents of one-time governance failure are reduced, the long-term systemic failures are more than just an isolated anomaly. Various experts and professional organizations dealing with risk management have come to the conclusion that the failures may be caused by a mess in the risk information due to different risk assessments from different perspectives (McCuaig, 2008, s. 3; Ernst, 2009, s. 4). The credit crisis and the resulting regulatory pressure forced the chief operating officers and senior management of financial services firms to focus more on risk convergence - the assessment, mitigation and reporting of risk. The process of organizing these risk assessments to provide the organizations with a more holistic view of the enterprise risk is fundamental to mastering risk assessment.

Before focusing on the different types of risk management frameworks, let us summarize the basics of risk assessment.

Risk assessment falls into the overall discipline of risk management. For most organizations, risk management is an evolving discipline that goes at disparate maturity levels across organizational disciplines such as internal audit, business operations, information technology and finance. Risk is defined as the uncertainty of an event occurring that could have an impact on the achievement of objectives. The definition of risk assessment then follows as the identification, evaluation and estimation of the levels of risks involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk (ISF, 2010).

Risk assessment should answer the following five questions (McCuaig, 2008, s. 3):

1. What can go wrong?
2. How can it go wrong?
3. What is the potential harm?

* University of Economics, Prague, Faculty of Informatics and Statistics (svata@vse.cz); Martin Fleischmann, Czech National Bank

This article has been elaborated with support from funds for institutional support to long-term conceptual development of science and research at the University of Economics, Prague, Faculty of Informatics and Statistics.

4. What can be done about it?
5. How can we stop it from happening again?

## 2. Emergence of risk-based approaches

Risk assessment is increasingly conducted by many groups within an organization to fulfil a variety of business and regulatory requirements. Various groups within the same organization often rely on guidance from different professional organizations to provide a framework for conducting the risk assessment. As these professional organizations offer disparate approaches to risk assessment, they contribute to a jungle of risk information. In this context, information systems and/or information technology (IS/IT) risk assessment plays an entirely exceptional role in each organization. There are two reasons for that statement. The first: IS/IT integrates all different functional areas within an organization and thus it has a potential to integrate the risk assessment activities as well; the second: IS/IT deals with data/information processing and as such by managing IS/IT risk we reduce the likelihood of "low quality" information. At the same time, we improve the quality of business processes, as information is the core part of each business process. Based on the assumptions, we can conclude that there is no need to make a difference between business risk and IS/IT risk. According to ITGI (2009), IT risk is business risk – specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. The business value and IT risk are two sides of the same coin and risk is inherent to all enterprises. So there is a need to manage all the risks. Yet, at the same time, seeking to eliminate all the risks, we can jeopardize the profit driving opportunities.

In practice, there is no single unified solution to the complex situation mentioned. Therefore, there are many different risk assessment frameworks aiming at different goals and different tools.

The incompatibility of various risk assessment frameworks can be recognized in three different aspects (dimensions):

1. depth of coverage of IT;
2. completeness of risk management scope;
3. level of balance between the risk-focused vs. control-focused approaches.

### 2.1 Depth of coverage of IT

Different risk management frameworks take into account the specifics of the IT area differently. COSO ERM, AS/NZS 4360, ISO 31000 and BASEL II are typical examples of not paying special attention to IT risk management. However, considering that Basel II is a very important standard for financial organizations, and at the same time these institutions introduce governance principles to their management systems, there is a need to integrate both the frameworks. In 2008, ISACA and ITGI introduced the document "Control Objectives for Basel II". It provides a framework for managing the operational and information risk in the context of Basel II. It presents an outline of risk under Basel II, the links between the operational risk and the IT risk, and an approach

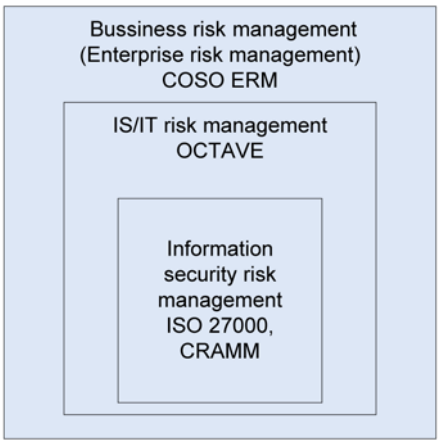
for managing the information risk. The document addresses three groups: information risk managers, IT practitioners and financial services experts. The executive summary states that financial services organizations using the framework presented are able to apply recognized IT control objectives and management processes to address the role of IT in operational risk.

On the other hand, focusing on the depth of the IT coverage within the risk management frameworks, we can furnish frameworks such as ISO 2700x, ISF and CRAMM. They are examples of frameworks covering IT risk management without any serious attempt to integrate it with the business risk management. The framework OCTAVE is the only framework which deals with organizational risk in addition to IT risk.

### 2.2 Completeness of risk management scope

Each enterprise has to deal with many different types of risks. Historically, the most serious risk is the business risk. Business risk roots penetrate many business sources: credit, strategic, market, competitive, operational, etc. The growing integration, globalization, complexity and dependence on IT has resulted in the emergence of other important types of risk: compliance, financial and technology. Each risk management framework applies a different approach to risk categorization. Even to our previous considerations about the close relation between business and IT risk, it is quite common to think about these types of risk separately. In Figure 1, the different levels (scopes) of risk management are shown together with examples of risk management frameworks.

**Figure 1**
**Different levels (scopes) of risk management**



### 2.3 Level of balance between risk-focused vs. control-focused approaches

Another problem arises when we start to analyze the relationship between risk and control. All the current frameworks are based on the idea that there is a need to distinguish among three main stages in risk management. The below example taken from ISF (2010) represents them:

- Business Impact Assessment – assesses the potential level of business impact and determines the security requirements for protecting information in critical business applications;
- Threat and Vulnerability Assessment – determines the likelihood of particular threats to exploit vulnerabilities and cause business impact;
- Control Selection – evaluates and selects controls to mitigate the threats.

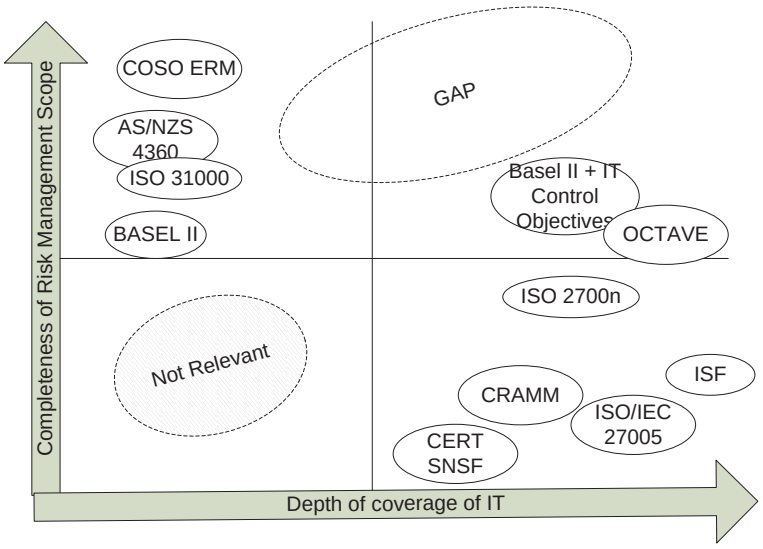
The final stage of the risk management process consists of "control selection", or in other words, "risk treatment" (ISO, 2008)[1]. Both the examples represent the final stage in each risk management process. The process should be understood as a cycle that is similar to the *PDCA* (*plan-do-check-act*)[2] model. The typical characteristic of each cycle is that there is no end or starting point. Therefore, the risk management activities can start either with control systems analysis or risk analysis. Again, different risk management frameworks handle this problem differently and in practice, many organizations struggle to find the proper balance between a risk-focused vs. control focused approach to risk assessment. For most organizations – especially financial ones – there is a bias towards control-focused risk assessment. The primary driver for this struggle is complying with regulations, such as Sarbanes Oxley and BASEL II, which originally drove the increased need for risk assessment. The need for compliance together with the need for auditing the internal control system forces organizations to focus on control-based risk assessment. Examples of such frameworks are COSO ERM, COBIT, and ISO 27002. These frameworks primarily refer to risk as the risk of missing or broken controls. On the other hand, when risk-focused frameworks (e.g. ANZ/NZS 4360, ISO 27005, and ISF) refer to risk, they refer to one or several responses (reject, accept, transfer or mitigate the risk). As a result, risk assessment teams use the same terminology with completely different meanings.

Different types of risk assessment frameworks are shown in Figure 2. Their positioning along the axis X – Depth of coverage of IT and axis Y – Completeness of risk management scope can help us understand both their relevance to the IT/IS area and the level of commonness in the understanding the phenomenon of risk.

1 Risk treatment covers four options to react on risk: avoid, transfer, reduce and accept the risk.

2 PDCA is an iterative four-step problem-solving process typically used in business process improvement. It is also known as the Deming cycle.

**Figure 2**
**International risk management frameworks**




Source: ISACA, 2009, s. 12.

Trying to summarize Figure 2, there is a whole range of different frameworks dealing with risk assessment, but these regulations either are too generic to be applicable to IS/IT risk management or, although they deal with IS/IT risk management, they narrow the area to IS/IT security risk management. The area named "GAP" identifies the space which is not well supported by the available frameworks, however, at the same time it represents the key to more integrated IT/IS and business risk management.

Table 1: The examples of the most popular frameworks for risk assessment (at the end of the text) offers a complete overview of the risk assessment frameworks.

With regard to filling the gap shown in Figure 2, it is worth mentioning especially the generally oriented initiative of these organisations called meaningfully *Risk IT.* In our opinion, the key contribution of this initiative is the fact that the framework connects business with IT risk management as closely as possible. This set of principles leads an enterprise to align its management of IT related business risk with its overall risk management. As such, it tries to bridge the gap in the current array of risk management frameworks for IT: there is no known framework that both includes a holistic look at risk management and, at the same time, provides an adequate depth and detail when covering IT. This might promote Risk IT as a unique tool offering a coverage that is missing in COSO ERM, AS/NZS 4360 and security-oriented IT risk management frameworks.

Risk IT complements ISACA's COBIT, which provides a comprehensive framework for the control and governance of business-driven, IT-based solutions and services.

**Figure 3**
**Risk IT components**


Source: ISACA, 2009, s. 15.

Risk IT contains two volumes:

1. *The Risk IT Framework* – Contains the guiding principles for IT risk management based on generally accepted standards. It includes a detailed and comprehensive process model which includes three domains, each comprising three processes (see Figure 3);and
2. *The Risk IT Practitioner Guide* – Contains practical guidance on how to manage IT risk.

Within the Risk IT Framework, the processes are structured much as in ISACA's Cobit and Val IT frameworks. The description of each process consists of:

- list of process management activities together with their narrative description;
- inputs and outputs of each activity (this approach is different from Cobit and Val IT, which include a model of inputs and outputs at the process level). The description is in the form of a table and enables understanding the major links between Risk IT processes;

- RACI Chart - Describes the roles and responsibilities (for each process):
  - roles under consideration are: Board, CEO, CRO3, CIO, CFO, Enterprise Risk Committee, Business Management, Business Process Owner, HR and Compliance and Audit;
  - responsibility designations:
    R – Responsible, A – Accountable, C – Consulted and I – Informed;
- goals and metrics (for each process) – Risk IT presents a top-down cascade of goals and metrics across the domain, process and activity levels. Goals define what the business expects, while metrics provide actual or potential outcome measures;
- maturity model – enables management self-assessment in response to the need to know what to do to achieve the best results. The maturity model is a popular and easy tool which can help managers do this job. In Risk IT, there is a maturity model available for each domain (this approach is again different from Cobit, which includes a maturity model at the process level). For each Risk IT domain, two versions of maturity models are provided:
  - high-level - Represents the same level of detail as Cobit (narrative description of the core characteristics for each level);
  - detailed version is built around the following attributes, each of which evolves through the levels:
    - awareness and communication;
    - responsibility and accountability;
    - goal setting and measurement;
    - policies, standards and procedures;
    - skills and expertise; and
    - tools and automation.

*The Risk IT Practitioner Guide* is divided into eight chapters and discusses topics such as defining a risk universe, how to define risk appetite, how to describe risk, how to develop relevant risk scenarios, how to respond to risk, and how Cobit and Val IT can assist in mitigating risk. The guide contains several templates, as well as a comprehensive list of generic IT risk scenarios (Steuperaert, 2009, s. 16).

Considering the typical financial institution, where an enterprise risk management approach (ERM) together with other frameworks (SOX, BASEL, ITIL, COBIT, ISO, etc.) have been established, but where IT risk management is treated and reported separately, the Risk IT process model can be used to start integration of IT risk management into the overall ERM system by assigning IT-related responsibilities to the roles defined in the Risk IT model and by implementing any additional process steps required as described by Risk IT's Risk Governance (RG) domain. This introduction of Risk IT Framework can be applied by most enterprises having an organized approach to risk management.

3 CRO – Chief Risk Officer.

## 3. Specifics of IS/IT risk management in banking industry

It is becoming increasingly apparent that information systems and technologies significantly influence business processes in the banking industry. The value of IS/IT depends widely on the way IS/IT are implemented and related to the banking activities. The IS/IT as such represent an important factor of competitiveness and commercial success of individual financial institutions.

IS/IT affect the banking business and its economic results in the following ways:

- contribution of IS/IT to the business productivity;
- making use of IS/IT as a tool for banking innovations[4]; and
- IS/IT as a banking risk mitigating (increasing) factor.

In accordance with the main focus of this article, we will hereafter highlight the relationship between IS/IT and risk. This role of IS/IT matters very much since drawbacks in risk control might lead not only to financial losses and a failure of individual institutions or threat to clients' deposits, but also to a negative impact on the whole economy both nationally and globally.

From this point of view, we can observe two relationships between risk management and IS/IT:

- IS/IT support risk management in banks, e.g., databases enabling recording and analysing of risk events, systems supporting models for risk quantification, credit scoring applications, etc.;
- IS/IT penetration into the banking processes causes dependency of business activities on IS/IT, which increases the significance of IS/IT risk management.

Risk management is an inseparable part of business on financial markets. The core of an efficient and effective risk management lies in determining an optimal level of risks that are to be tolerated whereas risks above this level are suitable to be controlled.[5]

The ability to find the right balance between an inclination to risk and a tendency to its elimination is the very way to reach stable economic results.[6] Therefore, investment in risk management does not automatically mean a negative item in a profit and loss statement, but it might (and should) significantly contribute to the profitability of a bank. A bank's economic result is thus a common denominator of the business activity on the one hand and an efficient risk management on the other.

With regard to the aforementioned dependency of business on IS/IT and due to the advanced stage of their penetration into the banking activities and products, the importance of IS/IT risk management is growing. This fact is reflected by banks themselves and obviously also by regulators. Leading regulators pay adequate attention to IS/IT in banks and many of them, including the Czech National Bank, have published prudential rules and carried out systematic supervision in this area. Regulatory requirements on

4 This is a factor of volatility and heterogeneity in the banking industry.

5 This is also referred to as risk appetite, risk tolerance or maximum accepted risk.

6 Tomáš Bat'a: The biggest science is finding the right direction between caution and courage.

IS/IT in banks reflect the unique role of the banking industry for the national economy, general principles of banking risk management and the importance of IS/IT in banking as such. Although this basis stresses the specifics mentioned above, IS/IT regulation complies with the best practices and generally respected standards such as ISO 2700x, COBIT, ITIL etc.

Except these general standards on IS/IT, there are other relevant frameworks specific to banking, Basel II being the most important one. This framework has promoted operational risk among the three main banking risks besides credit and market risk, thus also highlighting IS/IT risk as an integral part (substantial subset) of operational risk. The Basel II definition of operational risk regards systems as one of four operational risk drivers; however, the coverage of IS/IT issues within Basel II is not deep.[7] Although Basel II sets down only general principles and methods for operational risk capital requirement quantification, it establishes operational risk management as a separate risk discipline. However, no global operational standard, including guidance for the implementation of a bank's operational risk framework and particular operational risk management methods, has been established yet.

There have been some attempts to resolve this situation. An example is the methodology RMA-KRI Framework[8]. This metodology is a product of the Risk Management Association, which in conjunction with Risk*Business* International Limited launched an initiative aimed at furthering the use of KRIs across the financial services industry. This followed the publication of several white papers by international rating agencies regarding the inclusion of operational risk effectiveness capabilities into an organisation's credit rating, as well as the publication of the then draft Basel II guidelines, which suggested that standardised indicators could be used to adjust an organisation's calculated capital reserve requirement under the Advanced Measurement Approach[9] (IOR, 2010, page 37).

Another approach to how IT risk management is treated within the banking industry is the implementation of the so-called Operational Risk Management Framework (ORM). The main aim of this framework is to rethink the way of risk management and integrate it with business processes. There is no "one-size-fits-all" approach to ORM. It is not merely Basel-compliant or Cobit-compliant, but it should also provide the bank with mechanisms for improving its overall risk culture and behaviour towards operational risk management. The concept of the ORM Framework is often supported by specialized software, which is periodically evaluated using e.g. Gartner Magic Quadrant[10] (Gartner, 201As concerns banks in the Czech Republic, the following paragraph tries to summarize trends regarding the application of the above mentioned frameworks and their integration into banks' general risk management strategies. The

7 This refers to the gap shown in the Figure 2 in chapter 2.3. and ISACA/ITGI initiatives to fill this gap described in the chapter.

8 RMA-KRI : Risk Management Association, Key Risk Indicators.

9 Advanced Measurement Approach (AMA) is a set of operational risk measurement techniques proposed under Basel II capital adequacy rules for banking institutions.

10 Magic Quadrant for Operational Risk Management Software for Financial Services.

overview is based on the author's long years of experience and knowledge in the field of the Czech National Bank's IS/IT banking supervision. It is necessary to mention that it is not a snapshot of a certain time because the Czech National Bank performs the IS/IT supervision in the form of on-site examinations, which requires a few years to go through the whole banking sector. Therefore, it is not possible to get complete numbers of entities employing this or that framework. Although the following statement does not represent an exact survey, it can certainly illustrate the knottiness of the situation.

The form of the ORM is determined by the CNB regulation that stipulates not only Basel II requirements on the ORM, but also specific regulation on IS/IT risk management.[11] These regulatory requirements are not understood as separate groups of principles. On the contrary, the CNB's regulation aims towards the integration of IS/IT risk into the overall ORM. However, the regulation stipulates the requirements in the form of general principles. It neither stipulates detailed rules nor makes banks apply particular IS/IT risk management standards. This gives banks a considerable room for their own way to comply with the regulations. As regards the ORM as such, its form and sophistication is determined primarily by the chosen approach of capital requirement calculation for operational risk, which leads to the use of different operational risk management tools. From this point of view, most Czech banks using or implementing Advanced Measurement Approaches (AMA) and several other banks reflect, to some extent, Basel II IT Control Objectives. This helps integrate their IS/IT risk management into their overall operational risk management frameworks. This linkage is more often initiated by IT people since they are more familiar with ISACA's frameworks. Although IT Control Objectives proved useful in banking practice, they do not fully cover the needs of IS/IT risk management. Therefore, most Czech banks use one or a combination of several IT-oriented risk management frameworks that have been adjusted and incorporated into their internal methodologies (in-house methodologies). The ISO 2700n family is the leading IS/IT risk management framework among Czech banks. Its implementation reflects the internal risk management processes including parent company methodologies. On the contrary, CRAMM, which used to be relatively popular, is no longer used as it proved to be too sophisticated and not flexible enough. Other IS/IT risk management frameworks are used singularly. Furthermore, ITIL is worth mentioning. Although it is not a framework primarily focused on IS/IT risk management, it reflects several security issues. Its significance lies in the fact that ITIL undoubtedly belongs among the most frequent IT frameworks in the Czech banking sector.

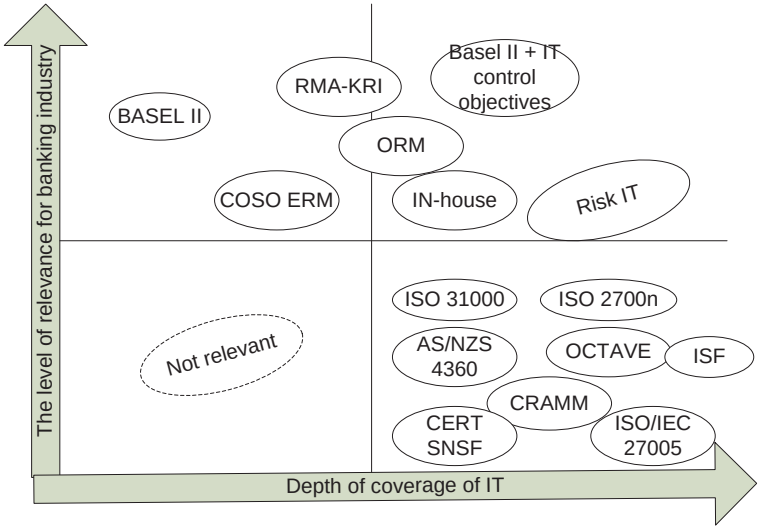
Figure 4 should help you roughly understand the level of relevance of all the above discussed frameworks to the banking industry.

The particular form of the methods thus remains vague, so the form of operational risk management differs from one bank to another and its unification advances mostly by experience. This state yields many possible combinations and as such it repre-

11 All EU supervisory authorities regulate operational risk management. Most of them also reflect IS/IT risk management in their regulations.

sents a great challenge for both banks and regulators. It makes IS/IT risk management integration into operational risk management frameworks more difficult.

**Figure 4**
**IT risk management frameworks for banking industry**




### 3.1 Depth of coverage of IT risk management in banking industry (Czech Republic)

Operational risk is a specific type of risk in comparison to the traditional banking risks. While credit, market and liquidity risks are derived from financial portfolios, operational risk is primarily related to processes (transactions) and as such it is an implicit risk. Unlike credit and market risks, operational risk requires decentralization and continuous involvement of business units.

Operational risk is defined as the risk of loss from inadequate or failed internal processes, people and systems or from external events. According to the Basel II definition, it includes legal risk, but excludes strategic and reputational risks.

The position of IS/IT risk within a bank's risk management framework should logically result from this definition and from the fact that IS/IT risk forms a significant subset of operational risk, which is attributed in particular to an increasing IS/IT penetration into the banking processes. As a large portion of the whole operational risk falls under IS/IT risk, it should theoretically be an integral part of the operational risk framework. However, the practice still frequently differs from this assumption, which is due to the following reasons.

**Figure 5**
**Elements of operational risk**


Source: Němec, 2010, slide 4.

The first one is a lingering barrier between IT and non-IT departments, where IT managers prefer to deal with "their" problems on their own on the one hand, and business management does not seem to be interested in "technicalities" on the other. Such a situation preserves differences between IT risk management and management of other risks including operational. It prevents us from looking for analogous features and upsets a convergence of risk management techniques. The other reason impeding the integration of IT risk management into the operational risk management framework is that authors of modern and currently used operational risk frameworks ignored the existence and long track record of IT risk management techniques. They ironically overlook the fact that these techniques are not only elaborated but also implemented and functioning. However, things are slowly but surely looking up as we can witness signs of a convergence of the above mentioned risk management approaches, e.g., by way of initiatives such as IT Control Objectives for Basel II (see Chapter 2.3). On the other hand, operational risk managers accept IS/IT as an important risk driver and mostly also understand its specifics. To some extent, they deal with the same issues as IT security managers. Examples may include physical security, business continuity, third-party issues, incident management, etc. The advanced measurement approaches (AMA) require and lead to considering all operational risk drivers, including IS/IT. Moreover, the four basic elements of AMA (internal data, external data, scenario analyses, and business environment and internal control factors) highlight the points of view analogous to the traditional IT – security-oriented frameworks dealing with assets, threats, vulnerabilities, impacts and probability. Therefore, we can find a lot of similarities.

Another considerable problem is that all elements of operational risk (processes, people, systems and external events) are present and relevant to risk management of

the aforementioned financial risks. It causes difficulties in determination of an unambiguous separation between operational risk and these risks, which is a hot and still intensively discussed issue.

### 3.2 Completeness of risk management scope and regulation in banking industry

A bank's risk management has to deal with two tasks:

1. to ensure compliance with regulatory requirements; and
2. to manage risks according to the risk appetite set down by executive management and stakeholders.

Ideally, there would be no difference between the aforementioned groups of requirements. However, such a state would apply only if both banks and regulators were perfect at risk quantification and at the ability to find the adequate level of risk tolerance and effective measures to control risks above this level. In other words, the regulation should ensure the banking sector stability, but not hobble its business on the one hand. On the other hand, a bank's risk management should ensure not only an adequate risk control, but stable economic results as well.

However, the situation differs in the real world. Banks tend to be as profitable as possible. Return on Equity (ROE) is one of the most important indicators for their stakeholders. From their point of view, having the highest ROE requires them to keep as little capital as possible, focus on selling products as much as possible and economize on expenses on non-business processes, including risk management. Such an approach might cause negative impacts ranging from losses to bankruptcy.

While banks stress the microeconomic point of view, regulators should take into consideration risks in the entire banking sector with regard to individual peer groups at most. Their main interest is the financial sector stability and as such they are supposed to be conservative in order to restrain excessive risk appetite. Although regulators usually have information about the banking sector in question and as such they can identify the main risks involved, they are not able to identify all the potential risks and quantify them exactly. This makes the regulatory role very difficult. Regulation may at best reflect available information and take into account identified risks.

However, in practice, there are other two factors that affect the final form and content of regulatory requirements:

- As regulation addresses a number of various institutions differing in size, range of activities, focus and organization, it should fit all entities so it sets down general principles rather than particular rules.
- The role of international regulatory standards is permanently increasing. It leads to a harmonization and codification of regulatory frameworks. We can illustrate this trend on the adoption of Basel II framework in EU law, which narrows the space for individual national regulators.

This state has its pros and cons. Principle-based regulation gives banks a wide range of risk management approaches and does not force them to keep many restrictive

rules. On the other hand, this makes getting assurance regarding compliance with regulation much more difficult. Another benefit consists in the fact that the current leading banking regulation[12] offers a compact framework, including a list of risks to be managed and a specification of methods, techniques and principles to be used.

Although this regulation implicitly assumes the necessity to manage IS/IT risk (as a subset of operational risk), IT risk is not mentioned as a risk discipline at all. Major regulators identified this important gap a long time ago. Therefore, they issued regulation on IS/IT in banks at the national level. They have also been performing supervision focused on this area for long. It has a logical implication that these national regulations are not unified and are differently integrated into the regulatory framework as such. In spite of that, we can find a lot of similarities not only concerning particular regulatory requirements but also with regard to the entire concept of IS/IT regulation. The reason is that advanced regulators are familiar with best practices and IS/IT (security) standards, are aware of the spread of their use in banks, see benefits related to their use for banks, and on that account, they tend to keep regulation in compliance with them. They predictably reflect especially standards addressing regulatory objectives that are typically formulated in IT security-oriented standards.

### 3.3 Level of balance between risk-focused vs. control-focused approaches in banking industry

The key interest of supervisory authorities is an assurance that the financial institutions in question carry out their business prudently. Prudent behaviour consists in being aware of taking risk, which requires the ability to:

- identify the risk;
- assess/measure the risk;
- monitor the risk;
- report about the risk; and
- control the risk (reject, accept, transfer or mitigate the risk).

The bank regulation typically deals with all the aforementioned risk management processes and combines both the risk-oriented and control-oriented approaches. It results from the fact that banks are under a regulatory obligation to quantify and allocate adequate capital to identified risks as well as to have in place controls in order to mitigate risks. Therefore, we can state that regulatory requirements for each risk management process usually encompass both points of view: risks and controls. Risk monitoring, for example, includes not only obtaining information about risk exposure but also check whether all the set controls are in place and effective.

12 The current regulatory framework for banks is represented especially by Basel II (including its transpositions in law).

**Table 1**

**Examples of the most popular frameworks for risk assessment**

| General Information[13] | Identification | Users | Target Organizations |
|---|---|---|---|
| • COSO ERM<br>• Committee of Sponsoring Organizations of the Treadway Commission<br>• www.coso.org/Publications/ERM/COSO_ERM | COSO issued Internal Control – Integrated Framework to help businesses and other entities assess and enhance their internal control systems. Recent years have seen heightened concern and focus on risk management. In 2001, COSO initiated a project, and engaged PricewaterhouseCoopers, to develop a framework that would be readily usable by managements to evaluate and improve their organizations' enterprise risk management.<br>COSO ERM views enterprise risk management as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. IT defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management. | • Executive management<br>• Internal auditors | All organizations that are to be compliant with strict internal control regulations:<br>• Sarbanes-Oxley Act for US SEC registrants and its affiliates,<br>• the Basel II framework<br>• the 8th Directive on company Law in the EU |
| • AS/NZS 4360:2004<br>• Standards Australia and Standards New Zealand<br>• http://www.standards.org.au/ | The standard provides a generic guide to managing risk and specifies the elements of the risk management process. The standard does not propose a uniform risk management systems, rather the standard proposes that the design and implementation of the risk management system should be influenced by the varying needs of the organisation, its products and services, and the processes and specific practices employed. | • Management | • Government agencies<br>• Large companies<br>• SME<br>• Commercial CIO<br>• Non-commercial CIO<br>• Specific sector: All sectors |
| • ISO 31000:2009<br>• International Organization for Standardization<br>• www.iso.org | ISO 31000 is intended to be a family of standards relating to risk management codified by the International Organization for Standardization.<br>ISO 31000:2009 has been received as a replacement to the existing standard on risk management, AS/NZS 4360:2004<br>ISO 31000:2009 addresses the entire management system that supports the design, implementation, maintenance and improvement of risk management processes.<br>Currently, the ISO 31000 family is expected to include:<br>• ISO 31000: Principles and Guidelines on Implementation<br>• IEC 31010: Risk Management - Risk Assessment Techniques<br>• ISO/IEC 73: Risk Management - Vocabulary | • executive level stakeholders<br>• appointment holders in the enterprise risk management group<br>• risk analysts and management officers<br>• line managers and project managers<br>• compliance and internal auditors<br>• independent practitioners | • Government agencies<br>• Large companies<br>• SME<br>• Commercial CIO<br>• Non-commercial CIO<br>• Specific sector: All sectors |

13 General information includes information about method or tool name, vendor and official web site.

| | | | |
|---|---|---|---|
| • ISO/IEC 27005:2009 (ISO 13335-2) Information security risk management<br>• ISO | Describes the complete process of information security Risk Management in a generic manner. The annexes contain examples of information security Risk Assessment approaches as well as lists of possible threats, vulnerabilities and security controls. It can be viewed at as the basic information Risk Management standard at international level, setting a framework for the definition of the Risk Management process | • Management<br>• Operational | • Government agencies<br>• Large companies<br>• SME<br>• Commercial CIO<br>• Non-commercial CIO<br>• Specific sector : N/A |
| • ISO Guide 73:2009 Risk Management Vocabulary International Organization for Standardization<br>• www.iso.org | Provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.<br>For principles and guidelines on risk management, reference is made to ISO 31000:2009 | • risk managers,<br>• those who are involved in activities of ISO and IEC, and<br>• developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk | • Government agencies<br>• Large companies<br>• SME<br>• Commercial CIO<br>• Non-commercial CIO<br>• Specific sector: All sectors |
| • BASEL II<br>• BASEL II and IT control objectives | Basel II is an international standard published by the Basel Committee on Banking Supervision in June 2004. It gives recommendations for banking regulators with regard to capital standards and risk management in banks. Basel II sets down risk and capital management principles to ensure a bank holds capital reserves appropriate to its risk exposure. It aims to make capital allocation more risk sensitive and gives wider range of approaches for risk and capital adequacy quantification. Unlike Basel I the Basel II framework includes operational risk (except credit and market risks). Basel II consists of three pillars: (i) minimum capital requirements, (ii) supervisory review process and (iii) market discipline. The EU adopted Basel II framework into the Capital Requirements Directive (CRD) that came into force on 1 January 2007. As a part of European law, it reflects the Basel II rules on capital measurement and capital standards.<br>IT Control Objectives for Basel II provides a framework for managing operational and information risk in the context of Basel II. It presents an outline of risk under Basel II, the links between operational risk and IT risk, and an approach for managing information risk. The executive summary states that financial services organizations using the framework presented are able to apply recognized IT control objectives and management processes to address the role of IT in operational risk. | • Stakeholders<br>• Executive management<br>• Management<br>• Risk mangers<br>• Internal auditors<br>• information risk managers<br>• IT practitioners<br>• financial services experts | • Banks<br>• Other credit institutions<br>• Regulators<br>• External auditors<br>• Rating agencies |



AOP 19(3), 2011, ISSN 0572-3043

| | | | |
|---|---|---|---|
| • OCTAVE Method<br>OCTAVE-S, OCTAVE-Allegro<br>• Carnegie Mellon University, SEI (Software Engineering Institute)<br>• http://www.cert.org/octave/ | OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.<br>OCTAVE Methods<br>There are three OCTAVE methods:<br>• the original OCTAVE method, which forms the basis for the OCTAVE body of knowledge<br>• OCTAVE-S, for smaller organizations<br>• OCTAVE-Allegro, a streamlined approach for information security assessment and assurance<br>OCTAVE methods are founded on the OCTAVE criteria—a standard approach for a risk-driven and practice-based information security evaluation. The OCTAVE criteria establish the fundamental principles and attributes of risk management that are used by the OCTAVE methods. | • Management<br>• Operational | • SME<br>• Specific sector: N/A |
| • CRAMM (CCTA Risk Analysis and Management Method)<br>• Insight Consulting<br>• http://www.cramm.com | CRAMM is a risk analysis method developed by the British government organization CCTA (Central Communication and Telecommunication Agency), now renamed the Office of Government Commerce (OGC). A tool having the same name supports the method: CRAMM. The CRAMM method is rather difficult to use without the CRAMM tool. The first releases of CRAMM (method and tool) were based on best practices of British government organizations. At present CRAMM is the UK government's preferred risk analysis method, but CRAMM is also used in many countries outside the UK. CRAMM is especially appropriate for large organizations, like government bodies and industry. | • Management<br>• Operational<br>• Technical | • Government agencies<br>• Large companies<br>• Specific sector: N/A |
| • ISF products:<br>1) The Standard of Good Practice for Information Security<br>2) FIRM (Fundamental Information Risk Management) and the revised FIRM Scorecard<br>3) ISF's Information Security Status Survey<br>4) Information Risk Analysis Methodologies (IRAM) project<br>5) SARA (Simple to Apply Risk Analysis)<br>6) SPRINT (Simplified Process for Risk Identification)<br>• Information Security Forum (ISF)<br>• http://www.securityforum.org | ISF products concerning RA/RM refer often to each other and can be used complementarily. The Standard of Good Practice is split into five distinct aspects, each of which covers a particular type of environment. These are:<br>• Security Management (enterprise-wide)<br>• Critical Business Applications<br>• Computer Installations ('Information Processing' in previous versions)<br>• Networks ('Communications Networks' in previous versions)<br>• Systems Development<br>FIRM is a detailed methodology for the monitoring and control of information risk at the enterprise level.<br>SARA is a detailed methodology for analyzing information risk in critical information systems.<br>SPRINT is a relatively quick and easy-to-use methodology for assessing business impact and for analyzing information risk in important but not critical information systems. | • Management<br>• Operational<br>• Technical | • Government agencies<br>• Large companies<br>• Commercial CIO<br>• Non-commercial CIO<br>• Specific sector: N/A |

## 4. Conclusion

The current financial crisis may be regarded as an opportunity to correct certain aspects of financial systems, namely those that had led to it. As the crisis proved to be very serious and has definitely not finished, its reasons are being intensively discussed. They are often identified as the shortcomings of risk management systems on the one hand and insufficient regulation on the other. Although this statement is not surprising and seems to be true, we doubt whether both the aforementioned aspects have been sufficiently analysed. In this situation, in our opinion, financial institutions and regulatory bodies should have provided a deep and thorough analysis of the current risk management systems, their effectiveness and efficiency.

Anyway, with regard to the topic of this article, the risk management systems in the banking industry have failed in many cases due to inadequate corporate governance procedures rather than the inadequacy of the IT systems as such. On the other hand, the entire corporate governance includes IT governance as well since business and IT are communicating vessels. An attempt at explaining these mutual relationships has been made in this article. Generally speaking, the supervisory boards and senior managers failed in their responsibilities for implementation and control of risk management systems. They very often approved their risk management strategies in a formal way without establishing suitable metrics and monitoring lines assuring that a risk management system is implemented in accordance with the strategy, up to date, efficient and effective.

In spite of that, the principal improvements in banking governance and risk management have not been significant. The banks that have survived do not seem to reflect the lesson much. This does not seem rational as we suppose that next time, they will not be able to rely on financial assistance from the state in the same extent as during this crisis. On top of that, the banking industry's risk exposure has not been reduced.

However, to be honest to banks' top managers, their role is not easy. This article introduced the risk management approaches, standards and regulations relevant for risk management in the banking industry with an emphasis on IS/IT risk management. Although the wide range of these frameworks seems to be an advantage, ironically it makes their effective use harder for a bank's management. The more approaches exist, the more complicated it is to choose the right ones especially when we take into account the above described differences between these frameworks regarding the completeness of risk management, depth of IT coverage, risk vs. control-focused orientation, and compliance with the regulation.

Banking regulation has generally been supposed to be the other cause of the crisis.

We have already noticed some activities in this field. The first example is the announcement of the Council of the European Union ("EU") that it has endorsed an agreement made with the EU Parliament on 2 September 2010 on reforming the EU financial supervisory framework. Another example is the Basel Committee's agreement on key design elements of the reform package. The preparation of the Basel III documents is an important part of this effort. The common aim of all these activities is to improve risk management and governance. However, we find these activities questionable as the establishment of the new EU supervisory body and the ongoing update of

the banking regulation have not been preceded by a fundamental analysis of the current financial crisis, including its reasons. In addition to that, each subsequent version of the regulation is becoming more and more complex. It makes its understanding, implementation and supervision very difficult.

We hope that this article can help the reader understand the core problems of risk management and, at the same time, choose the most appropriate framework to resolve these problems.

## References

ERNST&YOUNG. 2009. Risk Convergence: The Future State of Governance, Risk, and Control.

GARTNER. 2010. The Gartner Magic Quadrant for Operational Risk Management for Financial Services. www.gartner.com/it/products/mq/mq_ms.jsp.

IOR, Institute of Operational Risk. 2010. Operational Risk Sound Practice Guidance Key Risk Indicators. November 2010. www.ior-institute.org.

ISACA. 2007. IT Control Objectives for Basel II - The Importance of Governance and Risk Management for Compliance. ISBN 1893209385.

ISACA. 2009. Risk IT framework. ISBN 978-1-60420-111-6.

ISACA. 2009. Risk IT Overview. www.isaca.org/Knowledge Center/Standards.

ISF, IRAM. 2010 https://www.securityforum.org/?page=DocumentView&itemid=4414.June 2010.

ISO 27005:2008. Information Security – Security Techniques – Information security risk management.

ISO 31000:2009. Risk management – Principles and guidelines.

ITGI. 2009. Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework, Exposure Draft.

MCCUAIG, B. 2008. Fundamentals of GRC: Mastering Risk Assessment [White Paper]. Thomson Reuters, 2008.

NĚMEC, M. 2010. Summary of methods used for management and measurement in AMA Banks and validation procedures. Presentation for the Czech Institute of Internal Auditors, October 2010.

STEUPERAERT, D. 2009. Identify, Govern and Manage IT Risk. *Cobit Focus.* 2009, October. www.isaca.org.

## IS/IT RISK MANAGEMENT IN BANKING INDUSTRY

**Abstract:** The paper makes a survey of current trends in business risk management focusing on IS/IT risk management in financial institutions. Special attention is paid to frameworks and regulations available for both financial and non-financial risk management and their relation to IS/IT risk management. The relationship and common and different features between IS/IT risk management and operational risk management are discussed on the basis of a short introduction to the specifics of risk management in financial institutions. The advantages and challenges of those different frameworks are summarized together with the possibility to incorporate some IT/IS risk management tools and methods into operational risk management in practice. Basel II is the main framework covering the area of operational risk management, therefore the paper focuses on the assessment of the impact and integration of the Basel II framework with IS/IT risk management ones.

**Keywords:** IS/IT risk, operational risk, Basel, COSO, Risk IT

**JEL Classification:** M15