Integrated Management System in Information Society

Petr Doucek, Lea Nedomová, Jan Klas

University of Economics, Faculty of Informatics and Statistics, Department of System Analysis,
W. Churchill sq. 4, Prague, Czech Republic; {doucek, nedomova, klas}@vse.cz

Process of managing organizations and firms has never been simple activity. Together with growing complexity of relationships in society is also increasing the necessity of understanding the core process of managing at higher level of complexity. Management is no longer single problem of individual managers and is becoming more and more multidisciplinary and interdisciplinary. In this context it is necessary to take into account both partial aspects of management process and the process as a whole. The approach resulting from above mentioned bases is named as “Integrated management system” (IMS). The IMS introduces complex and sectional view of managing the firm. As being usual nowadays, it is based on process view both on core activities of organization (core processes) and on supporting processes including managerial processes. IMS comprises nowadays in particular of following areas of management:

- quality management,
- environmental management,
- occupational health and safety management system
- IS/ICT security management.

Key words: Integrated Management System, Quality Management, Environmental Management, Occupational Health & Safety Management System, IS/ICT Security Management.

Integrirani sistem managementa v informacijski družbi

Proces upravljanja z organizacijami in podjetji ni bil nikoli preprosta dejavnost. Skupaj z rastočo kompleksnostjo odnosov v družbi raste tudi potreba po razumevanju temeljnega procesa upravljanja na višjih nivojih kompleksnosti. Upravljanje ni več problem zgolj posameznih managerjev, pač pa postaja vse bolj multidisciplinarno in interdisciplinarno. V tem kontekstu je potrebno upoštevati tako oba delna vidika procesa upravljanja kot tudi proces kot celoto. Pristop, ki izhaja iz zgoraj omenjenih temeljev, se imenuje "integriran sistem managementa". Integriran sistem managementa vključuje kompleksen in delen vidik upravljanja podjetja. Danes običajno temelji na procesnem vidiku tako pri bistvenih dejavnostih organizacije (bistveni procesi) kot pri podpornih procesih, vključno z managerskimi procesi. Integriran sistem managementa obsega danes še prav posebej naslednja področja managementa:

- management kakovosti
- okoljski management
- zdravje na delovnem mestu in management varnosti pri delu
- management varovanja informacijskih sistemov in informacijske in komunikacijske tehnologije.

Ključne besede: integriran sistem managementa, management kakovosti, okoljski management, sistemski management varovanja zdravja in varnosti pri delu, management varovanja informacijskih sistemov in informacijske in komunikacijske tehnologije

1 Introduction

Today’s world is changing very fast. Nearly every day we can hear about new discoveries, about development in technologies, which are organizations forced forever to newly implement not to loose their position, it is concerning also changes in society itself. New products are constantly introduced to market and every day we are overwhelmed with amount of information from vast resources, etc. And exactly this world is being called with various attributes, like turbulent times or information society. In such situation in current global world, where the necessity of system management of all processes taking part in organization is growing more and more, was born the new philosophy of managing organizations – integrated management systems (IMS), which represents complex and sectional view of managing the firm (see Figure 1). Process of managing organizations is necessary to under-

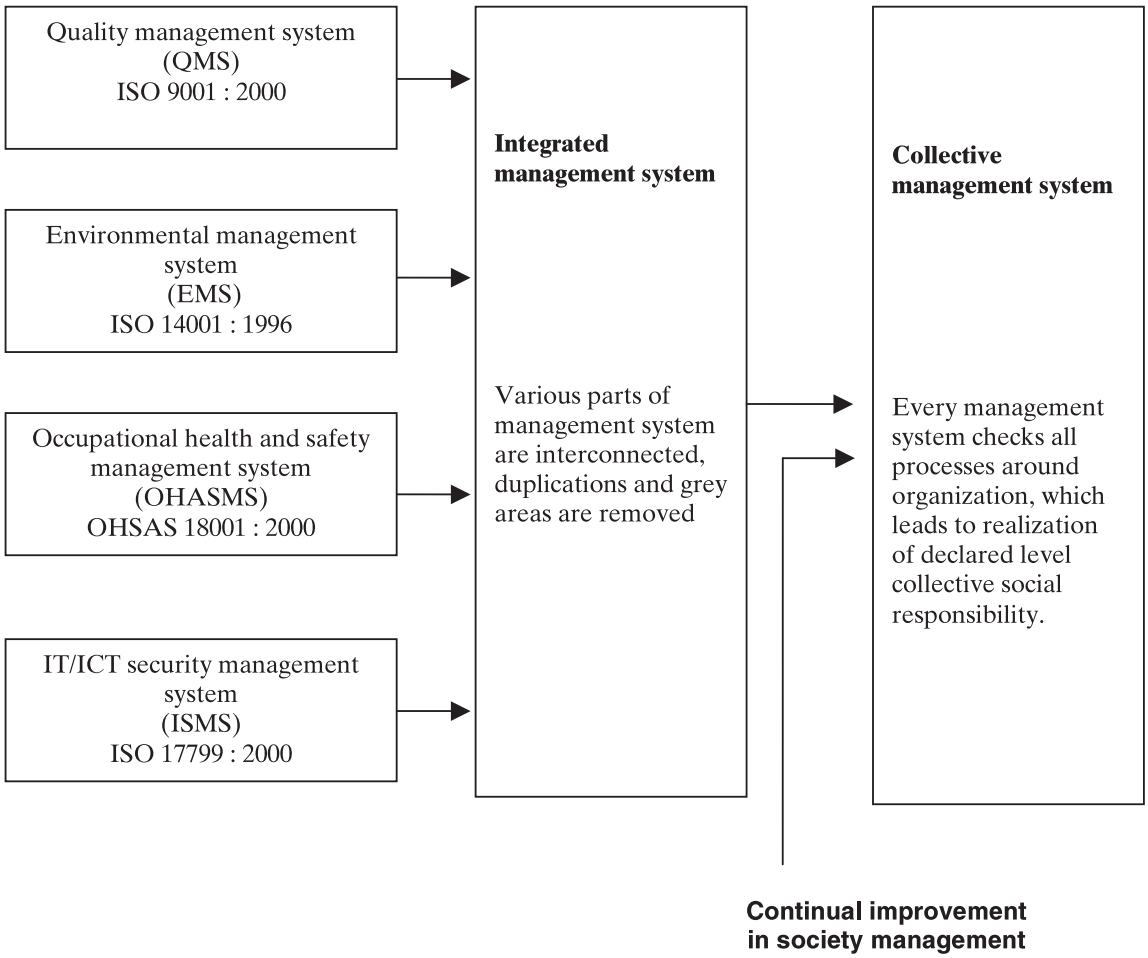

Figure 1: Integrated management system

stand as a complex problem. It is essential to manage even partial aspects of the whole process in its framework. Integrated management systems efficiency is evaluated by assessing compliance with accepted normatives. Normative requires all elements of these steps for their areas to be documented, which is the condition for sustainability. The most important benefit of international norm is their being systemic code of practice how to do things right – respectively according the best practice, which grew up in various parts of the world and which established themselves in praxis.

The components of integrated management systems nowadays constitute especially of following areas of management:

- quality management,
- environmental management,
- occupational health and safety management system
- IS/ICT security management.

Standards for management systems in these areas were developed by International Standards Organisation (ISO). These normatives are continually revised, usually in five year intervals, but still stay the methodical code of practice how to do thing right. They have uniform format with shared language and methodology and they also comprise continual improvement of management systems in organization.

Management system is always cyclical and consists of sequence of repeating steps:

- Announcement of particular commitment – policy of the firm
- Planning
- Implementation and operation
- Audit and correcting actions
- Evaluation of management process – review by management.

As it is obvious from above mentioned points, this is application of Deming's process model PDCA: Plan, Do, Check, Act.

2 Quality management

Phenomenon of quality has been crucial for enterprising sphere for several years. Managers are aware of quality being a constant (which customer always values) in ever-changing marketing conditions. Quality management in firm is one of the most important parts of enterprise management.

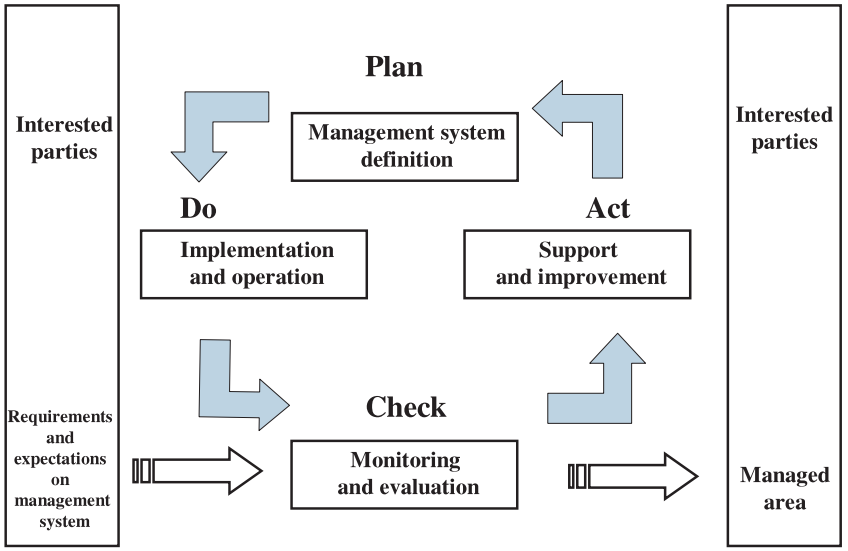

Figure 2: Illustration of Demming's PDCA model

Importance of quality comes from several reasons, first of them is that the quality is requested by nearly all customers and brings competitive advantage to firms. The second reason for managers is the order, respectively ordered system. Quality system is connected with prestige of firm, which presents its certification in advertising materials. Therefore quality is very important factor of firm, which takes its part in success or fail of the firm.

The importance of quality will be henceforward growing. Nowaday, in selection processes, it is part or even a condition in demand, if the potential supplier has implemented one of quality management systems. That means the suppliers without implemented system are in disadvantage. Moreover, some supplies are bound by law that suppliers have to have implement quality management systems.

2.1 Quality system instruments

Managing quality via checking parameters at stage of finished products, spread out in fifties and sixties, has been replaced with management orientation on processes in seventies. First had been production processes and other ones followed later. Meanwhile remains, that product quality defined with set of parameters is implicit criterion, which has to be met.

Customer orientation from then end of eighties brought the knowledge, that the one, who is deciding about quality of process/service, is the customer. Enterprises had to react to this situation with reengineering their processes, especially marketing process, which has to identify situation and provide management with news necessary for right and in-time decisions.

Functional structure, as the proven way of organizing, was no longer acceptable. It has been necessary to re-orientate to process management, where the crucial point is the goal, the assignment of process, with which has the procedure of process to mactch.

The primary task is the ability to win the customer and the ability to retain the customer. Ideal process procedure will keep the minimal amount of cost necessary for the process realization. Identification of all processes is the necessity for purposes of process management.

Nowadays there exists whole bunch of quality management systems, which differ in scale, number of implementations and also in area of application. Among the most known quality management systems instruments belong ISO norms of line 9000, applied mostly in Europe and the quality system TQM spread in Japan and America.

Furthermore it is possible to name systems for area of ecology, ISO norms of line 14000, systems for NATO suppliers AQAP, systems for pharmacy and laboratories GMP, GLP, systems of modifications ISO 9000 intended for various sectors and various countries like VDA 6.1, QS 9000 and many others.

2.2 Why to implement quality management systems?

The idea to implement quality management norm usually comes from assumption that purchasers will require that products they are purchasing have certain quality and that the quality has its standard in time. Further more because:

- it is required by key customers,
- firm aims to make order, improve productivity,
- it is competitive advantage, success of enterprise on market,
- it is good base for continual quality improvement,
- superior relationships with suppliers,
- mutual trust,
- superior contracts,

- firm is required by law.

Plan of quality management system implementation of specific firm will differ, or respectively will have different contents. More simple it will be within established firms, more detailed within firms with shorter existence.

Important is the participation of employees in preparation work for certification under leading of advisor, via preparating directives and other forms.

Implementation steps will be probably as follows:

1. Evaluate of actual state of quality management system in firm – create plan and select advisory firm.
2. Establish team for implementation – quality managers.
3. Perform introductory audit, which aims for detection of deficits regarding the norm and design procedure of implementation.
4. Define areas, in which it is necessary to create directives and allocate responsibilities for their creation.
5. Build quality management system in firm and educate top-management, quality managers.
6. Employees create working directives.
7. Perform internal audit by educated employees. Aim of these audits is to verify what has been stated in directives.
8. Adopt corrective actions in case of differences.
9. Select firm, which will conduct the audit and provide certification. For example following aspects will be of influence:
   - ❑ firm, which will conduct the certification, has to have accreditation for certification of particular production,
   - ❑ price for conducting the certification,
   - ❑ management decision to support national firms.
10. Prepare official version of directives after the internal audit and prepare pre-audit verification with certification.
11. Following results of verification and detection of deficits, design corrective actions after consultation with certification body.
12. Conduct audit with aim to obtain certification.

2.3 ISO Standards for QMS

Nowadays the basic and most well-know form of instrument for effective support in area of quality management, therefore such features of products (including services) which customers require, is quality management system (QMS) created according to norm ISO 9000:2000. This standard is flexible and sustainably able to absorb new and new market requirements. It is widely accepted standard and it is often considered to be keystone in qualities on which are later applied some extending norms. EU considers sustainable development of quality management systems to be the crucial condition of growth in ability of European industries to compete on the world market, which is documented also by announcement of so called programme of European quality support.

Norms ISO line 9000 are international standard, which has been introduced to market in the year 1987 in Geneva and several times updated (ISO directives set that norms have revised periodically in order to ensure that these norms are actual and are reflecting needs of society). The last update of these norms in 2000 emphasizes needs:

- monitoring customers satisfaction,
- fulfilling need of having documents, which are optimal for user,
- ensuring consistency between requirements and directives on quality management systems and
- supporting usage of generic rules of quality management in organizations.

Even though ISO 9000 is not mark of quality, its implementation in firm brings together aside from lower non-quality production also increasing trust of customers to firm and increasing firm culture.

The basic factors, which influence successful implementation of quality management system, are:

- understanding of quality,
- quality policy,
- quality management strategy,
- organization of quality,
- cost on quality,
- quality management system planning,
- quality management system implementation,
- team work,
- continual education, improvement of quality management systems and implementation.

The basis for revised norms, which are better united with philosophy and aims of most quality prizes programs, are eight rules for quality management:

- customer orientation,
- leading style - example of top managers,
- process approach,
- system approach to management,
- continual improvement,
- fact-based approach to decision-making,
- mutual advantageous supplier relationships.

These rules are clearly explained in ISO 9000 and in ISO 90004. Even if these rules make the basis of ISO 9001, they are neither appearing in this norm nor are part of its requirements.

2.4 Process approach

Quality management system described in revised norm is based on quality management rules, which comprises process approach. New structure (based on process) is consistent with PDCA improvement cycle, which was used also in norms of package ISO 14000 for environmental management system.

Process is every activity, which accepts inputs and changes them into outputs. The output from one process is often input into another process. Process itself is transformation, which adds value. In every process are employed people or other resources. The output can for example invoice, software, liquid fuel, banking service or final product or semi-product. It is possible to perform

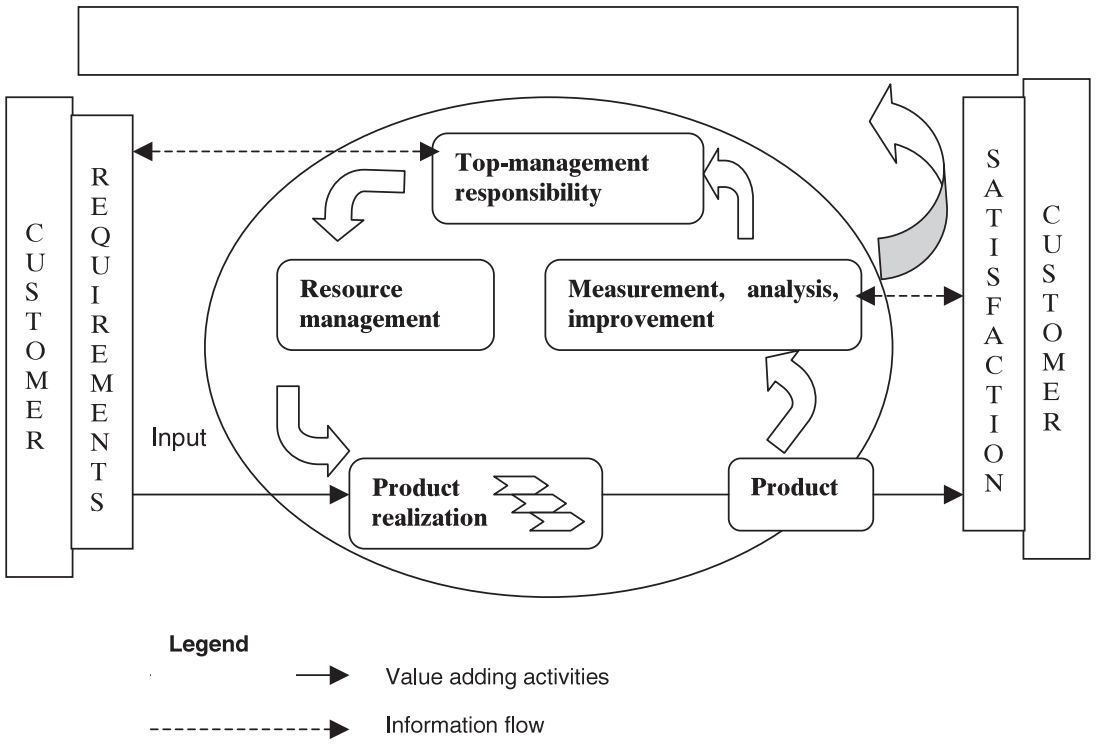

Figure 3: Model of process approach. Source: adopted according to ČSN ISO/EN 9001:2000

measurement at inputs and at different places of process and even at its output.

To be able to function effectively, organizations have to manage many mutually interconnected processes. International norms of line 9000:2000 encourage to adoption of process approach in organization management.

In the picture there is emphasized important fact, characterising revised issue of norms, that all processes in organization are being unwinded from customer requirements (and in really advanced organizations not only from requirements of customers, but also requirements of employees, owners, suppliers and organization's representatives), therefore interested parties and successfulness of the processes is again measured with rate of satisfaction of these interested parties.

This way framed system (Nedoma & Nedomová, 2002) then brings (to its product or service) added value, which can be perceived by:

a) Customers and end-users in form of:
   - ❏ fulfilling their requirements – reliability,
   - ❏ accessibility in the right moment – maintainability.

b) Workers inside organization as:
   - ❏ better working conditions,
   - ❏ more work satisfaction,
   - ❏ higher occupational health and safety,
   - ❏ better ethical approach,
   - ❏ stability of employment.

c) Owners and investors:
   - ❏ increased return on investments,
   - ❏ better production results (like productivity, time response, ...)
   - ❏ greater market share,
   - ❏ increasing profit margin.

d) Suppliers and partners:
   - ❏ relationship stability,
   - ❏ growing range of cooperation,
   - ❏ satisfactory partnership.

e) Society as:
   - ❏ guarantee of sustainable development of society via taking into account legal and ethical societal requirements,
   - ❏ increasing guarantees of occupational health and safety,
   - ❏ decreasing unfavourable effect on life environment.

3 Environmental management and audit (EMAS)

Organization's process management system, targeted on relationship between organization and life environment, is strategic instrument for creating trust of environment to organization and is "denomination" of organizational lifestyle and clear manifest of organization to the environment about its behaviour and approach to life environment.

Requirements on enterprise management from the point of view of life environment is feasible to fulfil with

implementation of next standardised enterprise management system, targeted on integrated prevention and pollution control and life environment preservation – the environmental management system (EMS).

For EMS are being usually applied two important international standards (Nedomová 2001):

- EMS according to international standards ISO line 14000 – this norm describes also supporting instruments targeted on EMS, services and evaluation of organization's environmental profile and its audit,
- EMAS (respectively EMAS II after revision no. 761/2001) – according directive 1836/93 EEC – scheme of environmental management and audit, valid in EU countries from Apr 13, 1995.

The abbreviation EMAS comes from simplified name of directive „Eco-Management and Audit Scheme". After few years of legal validity of its directive no 1836/1993, EU re-evaluated accepted procedures and considered acceptance of further directives, which can help substantially increase number of enterprises, which take into account management impact on life environment, strictly abide all legal directives in area of live environment, publish their report on life environment situation and on corrective actions, which they designated in area of life environment; these enterprises continually improve their relationship to life environment. Important is also that those enterprises, which already implemented this management system, are becoming more visible.

The question is, if normatives provide enough inspiration in sense of foresight, nevertheless the vision is set and normatives are useful system enabling change and routing organization to designated goal, to collective management of economy and preservation of life environment. Acceptance of both normatives is for organizations voluntary. The target is mostly integration of environmental aspect in management system and their continual improvement according to the following rule: Plan – Do – Check – Improve.

The aim of both normatives is to reach the designated targets, not only their announcement. Fulfilling ISO 14001 or EMAS requirements would not be only formal.

EMAS require, in difference to ISO 14001, validation of implemented management system and published so called public declaration, verified by EMAS certifier. Public declaration contains enterprise goals regarding life environment preservation including time horizons, in which the enterprise is bound to reach them. Public has with validated EMAS the opportunity: first to get information about enterprise's aims in area of life environment and second to check, how enterprise fulfils its commitments in area of life environment preservation.

EMAS is being preferred both in EU and Czech Republic. EMAS is in compliance with world trends to manage and influence life environment quality via employment of public into decision making process, based on free access to information.

From the new directive (EMAS II) results, that program EMAS is now open for all enterprises and organizations, which are willing to improve their environmental profile. Enterprises and services should be encouraged to voluntary participation in EMAS program, while they should benefit such participation, in areas of:

- legal control,
- cost saving,
- public image.

Next important aim of the new directive is that in EMAS program should take part also small and medium enterprises, whose participation should be supported by:

- simplifying access to information to existing supporting funds and to public institutions and
- creating or supporting actions relating to technical support.

Next important steps in increasing management system quality is processing and publishing regular report on state of life environment, which should public and other participating bodies provide with information on impact of their activities on life environment. Special importance is attached to these elements:

- compliance with legal norms,
- improving the overall impact of organization on life environment,
- employment of employees into management system,
- support of the partnership principle of participating bodies.

The EMAS program is now open for all sizes of organization and enterprises, which are willing to improve their environmental profile and its aim is enforcement of continual improvement of enterprise environmental profile via:

- EMS implementation and setting environmental policy and program relationship to place of action of enterprise,
- systematic, objective, and periodical evaluation of EMS effectiveness,
- providing public with information about EMS functioning.

Management system depicted in both EMS normatives is cyclical. The cycle begins with announcement of environmental policy. Then follows plan how to implement such policy. Proceeding to designated targets is continually rechecked and in case of necessity corrected. Management of organization periodically evaluates effectiveness of programs and efficiency of announced policy and plan. At the end of each cycle there is new beginning with new or amended environmental policy a plan, prepared on the basis of performed evaluations.

Schematically is the whole process of EMS implementation in organization (enterprise) illustrated in the following picture (Figure 4).

3.2 Why to implement EMS?

Among basic motivations for implementing environmental way of management belong motivations:

- to improve and simplify management system,
- to realize savings in material and personal resources,
- to improve the overall image of organization to public; organization is no longer personification of threat

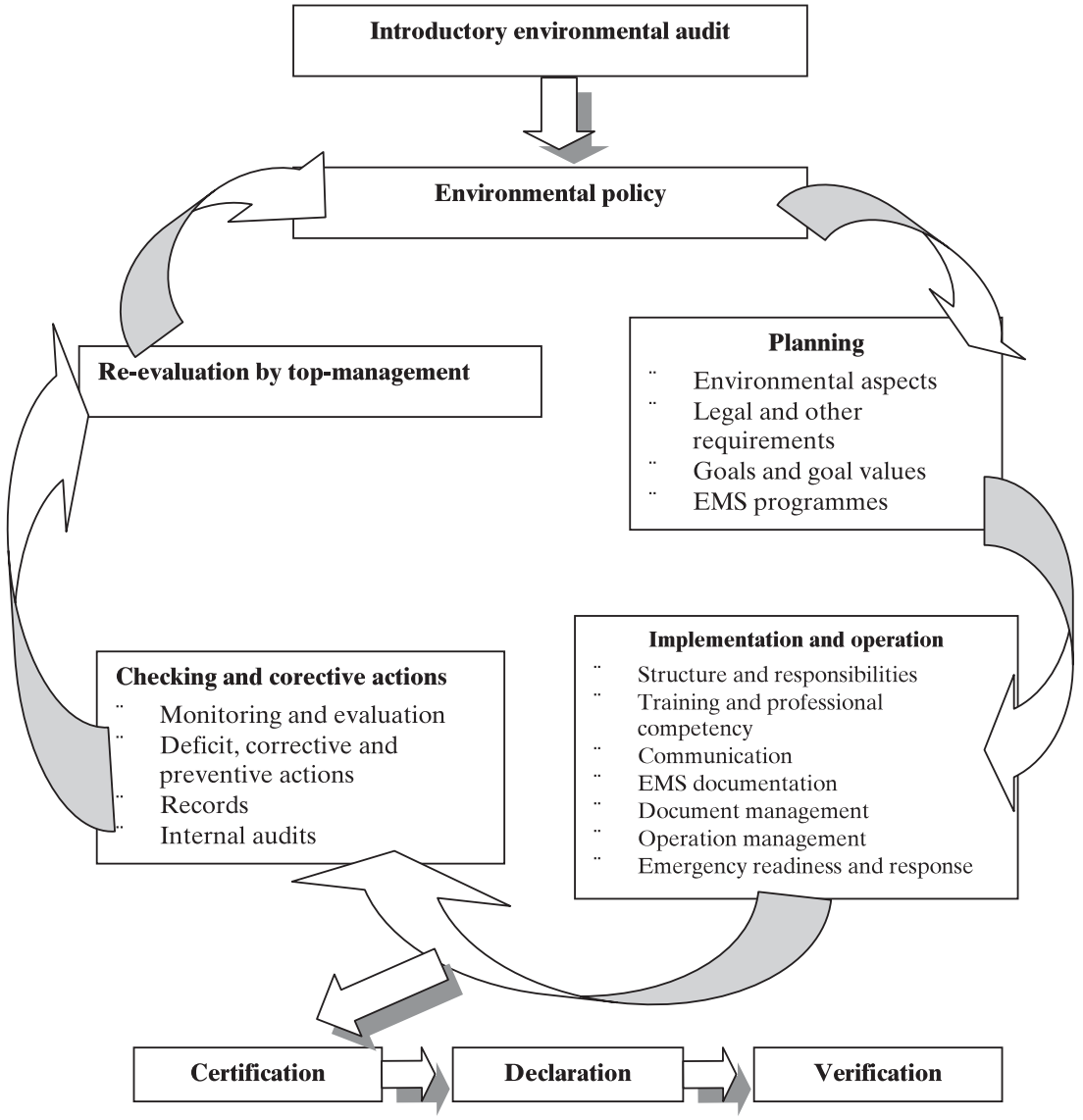

Figure 4: Graphical illustration of EMS implementation. Source: adopted according to ČSN EN ISO 14001 : 1997

potential and becomes trustful and reliable partner for its environment,

- to increase competitive ability; to make easier creating new markets and retaining the existing ones; to anticipate „green" alternative of outside pressure from the side of customers,
- to harmonize economic, environmental, social and legal aspects; to balance individual aspects with potential to influence decision making process and in advance to prepare on changes in legislative environment,
- to realize sustainable development of enterprise,
- to get prospective higher financial gains.

The main threat is only formal adoption of system, when the enterprise can conservate such practices, which are really not desirable from the point of sustainable development, so system can become contraproductive. Even the certified system EMS according to ISO 14001 itself doesn't tell anything about what is the behaviour of enterprise to life environment. In norm specified requirement of continual improvement is possible to relate only to improvement in EMS, which doesn't have to result in improvement in environmental profile and therefore to decreasing impact of enterprise activities on life environment. The concept of continual improvement can have various interpretations and it is important, how is this concept interpreted by enterprise and how by certification authority.

3.3 Relation to quality management system

Requirements on EMS, specified by international norms of line ISO 14 000, share rules of management with norms

of line ISO 9 000, but are not targeted only on individual customer, that means purchaser of the product or service, but are responding to whole-society need for life environment preservation and rules of sustainable development.

Experience shows that enterprises, which operate quality management systems, will more easier build EMS contrary to those, who haven't adopted this system. In their case it is advisable at maximum possible level to use existing structure and documentation as basement for EMS. First it is necessary to evaluate positive and negative experience gained during implementation of QMS.

Enterprise can utilize proven procedures and methods of creation documentation structure and its management, process management, training and internal audit. Therefore the chosen way of EMS implementation should absolutely take into account common areas of both systems in way, that there is not created any abundant parallel structure (Table 1).

Factual conflict arises in case, when to QMS is subordinated only to partial production unit. Via EMS it is necessary to spread this management system to the whole enterprise, because requirements are related to all localities, where are operated industrious activities managed by enterprise on given place. Even in case, that in area of QMS were already taken into account activities with important environmental aspects, they are not being considered as „environmentally important".

Table 1: Comparison of goals in QMS and EMS

QMS	***EMS***
Quality policy	Environmental policy
Quality goals	Environmental goals
Commitment	Commitment
Training	Training
Quality documentation	EMS documentation
Internal audits	Internal audits
External audits	External audits
Corrective actions	Corrective actions
Re-evaluation	Re-evaluation
Continual improvement in quality processes, products, and services	Continual improvement in environmental behaviour

Source: Nedoma & Nedomová (2002).

In advanced countries, there is implementation of environmental management system taken into consideration by, for example, insurance companies, somewhere there is lower taxation, more favourable credits or lowering fees for polluting the environment. These all then leads to increase in level of competitiveness, because firms with implemented EMAS system are in better position on market.

Standards enable to search all known sources of possible negative impact of production enterprise on life environment, asses the importance, adopt real actions in order to lowering their influences and evaluate results achieved.

Success of system depends on declared commitment and on employment of workers on all stages, including top-level management.

Implementation of EMS for sure improves management of production unit, both in holistic view (integration of life environment aspects into management), and in area of live environment preservation. Nearly in all cases there are also positive economic results (e.g. savings in material resources, energy, improvement in prevention of accidents, loss prevention, etc.) and non-economic (better documentation, increase in relationship with governmental bodies and public, etc.) Formalized prove of EMS implementation is then the certificate.

Enterprises and organizations are free to pay their initiative and to start building environmental management systems, to join the world-wide trend of decent ecological behaviour.

4 Managing occupational health and safety at work

Preservation of occupational health, life environment and assets before negative influences of manperformed economic activities is the target area of Occupational health and safety management system.

Guarantee of all requirements on occupational security is possible only with certain system. This system should enable:

- Identification, elimination or reduction of unnecessary or not acceptable risks.
- Ensuring following occupational health and safety rules and setting evaluationable goals in future.
- Ensuring following occupational health and safety at external firms, if possible in way that reduces company costs.
- Benchmarking and audit with independent provider. That means with whom, who has with the advantage of external view to find reserves and weak points in system.
- Flexible reaction on proceeding changes (e.g. legislative ones).

Occupational health and safety management has its own specifics, but is related to EMS, with which have common points. Occupational health and safety management should be in organization implemented because of reasons:

- Legal.
- Ethical.
- Employment law relationships.
- Financial.

The most spread and evidently most well-known instrument for the area of occupational health and security management at work is nowadays the directive OHSAS 18001 (Occupational Health & Safety Assessment series). This directive, which was issued as standard of well-know certification authorities, was last time

revised in November of year 2002. This norm is designed to be applicable for organizations of all types and sizes and is linked up to norms of line ISO 9000:2001 and of line ISO 14000:1997 so it is possible to create integrated organizational management system based on process approach model PDCA.

Building management systems of occupational health and security according to requirements of this directive should ensure that the organization satisfies all legal (and other) requirements on occupational health and security management. Level of detail, range of documentation and amount of resources for implementation of this system depends on size of organization and range of products and services offered. Organization itself can set if it will implement the system in whole organization or in area of particular production units or activities of organization. The basis of this system is establishing occupational health and safety at work policy, which clearly defines global goals in area of occupational health and safety at work and introduces leadership commitment to continual increase in level of occupational health and safety in organization.

When firm has already implemented quality management system or environmental management system reflecting ISO standard, then it is suitable and efficient to implement OHSAS 18001 requirements into already existing structure and to create this way the integrated management system, which will have following features:

- Integrated system must be covered with one leader – one coordinator of integrated management system.
- Firm policy and resources allocation is in unity.
- Organizational structure and responsibility allocation respect all integrated systems.
- Integrated systems also respect firm activities organization.
- Firm management and planning mechanism are harmonized, unified documentation is created (optionally unification harmonogram is elaborated).
- Information and support system, including maintenance and implementation of legal acts in firm, is harmonized.
- Training, education and reward and valuation system is harmonized.
- System of measuring and monitoring, including communication and reporting is simple.
- System re-evaluation, including planning and conducting internal audits is integrated.
- Corrective and preventive actions are unified.

Such system will be in praxis challenging to implement and organize, but brings documentation transparency and better coordination of activities inside whole organization.

Even in case, that firm has not implemented even one of the integrated management system parts, must comply with legal requirements on area of managing occupational health and safety. Basic legal acts in this area are reflecting requirements of general EU directive 89/391/EEC and relevant directives. In UK there is being used national norm BS 8800:1996.

For example, in Czech Republic there is possible to use in area of occupational health and safety the programme Safe enterprise, which is based on principles and rules set for occupational health and safety management systems by document OHSAS 18001, reference book ILO – OSH 2001 and also is in harmony with principles and rules applied by system norms - ČSN EN ISO 14001 and ČSN EN ISO 9001. With its requirements it is compatible with requirement of these documents on record management and cyclical management system in accordance to PDCA approach. Membership in programme is voluntary and the programme is intended for large and larger medium enterprises (http://www.cubp.cz). Because of efficient management of occupational health and safety area, there is formulated National Policy of Occupational Health and Safety in Czech Republic. Its implementation and evaluation is performed by the advisory body of Czech Government, which is Government Council for Occupational Health and Safety.

5 Information system a information and communication technology (IS/ICT) security management

The problematics of IS/ICT security itself is very large area, so let's focus on its control and audit. IS/ICT control and audit represents organic part of ensuring IS/ICT security process in organization. Their processes are directly connected with implementation of certain level – standards – of IS/ICT security in organization and in long term ensure, that the required (set) security level will be also kept.

The first group of problems, which de facto precedes the audit work itself, is setting the IS/ICT security level in organization. We will not primarily concentrate on ways and possibilities of setting security levels in organization, but these are similar to verification of ways of their abiding – certification or audit. Generally, security level both of product and information system is possible to implement in accordance with international standards - especially (ČSN 36 9789 - ČSN/ISO/IEC 15408), (ISO/IEC 17799), and (ČSN 36 9790 - ČSN/ISO/IEC 17799) – like mosaic of requirements on fulfilling certain security parameters and guarantee rate of their fulfilment. Guarantee rate of fulfilment is also part of the mentioned international standards – e.g. ČSN 36 9789 - ČSN/ISO/IEC 15408, ISO/IEC 17799.

Next area is the execution of own IS/ICT security control and audit. Procedures, which are in this case being applied, are possible to divide into following groups:

- product evaluation and certification according to ISO/IEC 15408, or prepared norm (ISO/IEC TR 19791 - ISO/IEC 17799) respectively,
- information system audit and certification according to ISO/IEC 17799,
- security incidents management in information system (ISO/IEC TR 13335-1-5),

- attestation of product and information system according to national standards.

Firm information system audit and certification according to ISO/IEC 17799 prefers managerial view on its security and concentrates on verification and compliance of information security management systems with this norm. The result is information system certification similar to ISO lines 9000 or 14000. This type of independent audit, when it is performed in full range, is concentrated on complex evaluation of information system including informatics system management and used especially in European commercial sector. Among potential deficits of audit according to this system is the approach to audit process itself and especially some of the used metrics. It happens very often, that used metrics – existence or non-existence of documents – are not capable to involve another dimension of this way audited documentation, e.g. its quality, content, up-to-date readiness, process meaningfulness, etc.

Evaluation and certification according to ISO/IEC 15408 (Common Criteria) is applicable for expressing security features of IS/ICT products. Nevertheless evaluation of product requirement compliance and real product feature is very demanding in time and used resource and because of that is number of so far evaluated and certificated products in some tens to hundreds. Because of reasons of evaluation comparison are set up specialized accredited certification laboratories and price for product evaluation in laboratories is very high. Even if the norms acknowledge evaluation of information system with help of this procedure, in praxis it happens very rarely.

Both abovementioned standards differ in some points substantially – mainly in targeted goal, and in some points they are on the other hand overlapping. Common Criteria (ČSN 36 9789 - ČSN/ISO/IEC 15408) and its extension (ISO/IEC 17799) accents especially compliance of product security features, while ISO/IEC 17799 concentrates on examination of product features as a whole – thus particular product installation in particular conditions.

IS/ICT security determination according to ČSN ISO/IEC 15408 is understood as elaboration of requirements on product based on mosaic in norm contained parameters, which must then satisfy evaluated subject (TOE) – Figure 5. This approach differs from original approach, which was represented especially by former security standards ITSEC and TCSEC. In them was IS/ICT security divided into classes and accomplishment of each security class constituted fulfilling exactly defined number of attributes. The disadvantage of this approach lies in that there is nearly flexibility in setting own priorities of IS/ICT. Approach specified in ČSN/ISO/IEC 15408 and in ISO/IEC 17799 Š6Ć enables to set own set of security attributes, level and rate of accomplishment satisfaction from the offered set. The set of offered attributes reflects basic processes in informatics and its operation management in form of criteria (attributes), which have to be accomplished for successful and safe organizational information system operation. Attributes are grouped into classes. Every class is always determined with its description and contains individual families of attributes. Family is determined with its behaviour description and also contains information on sorting its individual components (component is determined with its identification,

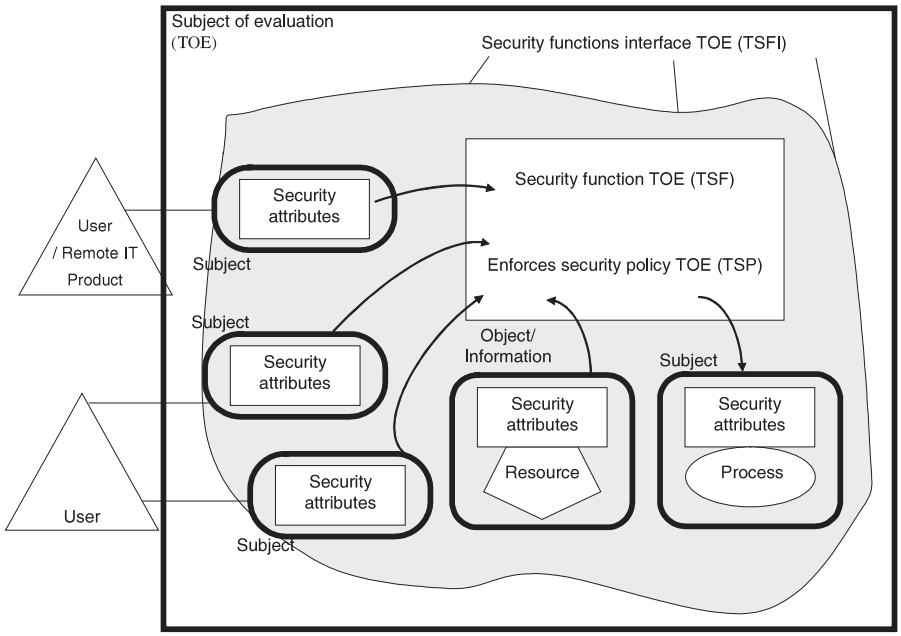

Figure 5: IS/ICT security approaches according to ČSN ISO/IEC 15408. Source: ČSN 36 9789 - ČSN/ISO/IEC 15408

functional elements – attributes and relationship among them) into levels, method of their management and method of conducting the audit. Scheme of ways of attributes determination is shown on following picture (Figure 5).

Further convergence of views on certification and audit IS/ICT security is the prepared international standard ISO/IEC TR 19791 – „Information Technology - Security Techniques - Security Assessment for Operational Systems". Standard – technical report – amends range of norm ČSN ISO/IEC 15408 for other aspects, which has mainly non-technological character. International standard ISO/IEC TR 19791 proposal broadens actually valid evaluation standard especially for following attribute families:

- personal security,
- configuration management, including security configuration management,
- security awareness,
- testing,
- documentation management, life cycle support. (Doucek 2004)

One of other important prepared international standards is ISO/IEC 18044 – Information technology - Security techniques - Information security incident management – which creeps the overall view on IS/ICT security questions management. The aim of standard is to:

- determine the most important categories of security incidents,
- set typological procedures of their resolution,
- determine roles in process of incidents resolution and together with them to set their authority and responsibilities.

Part of the standard is exemplary documentation for security incidents documentation. Standard proposal is possible to evaluate as important step, which creeps the overall view on information systems security management. Primarily it is targeted on large organizations, but even small and medium firms can drive inspiration in area of security incidents resolution from this standard.

Independent IS/ICT security verification and audit is important element of information security, which allows to deepen trust among producers and users of information a communication systems. Third independent party performing security verification plays role of independent arbitrator and helps in find suitable compromises.

But independent verification does not mean unified – or the more unified in the whole world. Because that problematic of security is domain of many experts in many countries with different cultural and societal background, there are in these countries also different "standards" of security evaluation. With their comparison is concerned international standard ISO/IEC PDTR 15443 („Information technology – Security techniques – A framework for IT security assurance"), respectively ISO/IEC PDTR 15443-2. The goal of this standard is to introduce methods and approaches to IS/ICT security resolution (products and information systems), to compare them among themselves and with standard ISO/IEC introduced in ISO/IEC PDTR 15443–1.

IS/ICT security becomes one of the most crucial success factors of investments in IS/ICT and the measure of their efficiency. In mediated role it becomes also the valuation of meaningfulness of firm's or institution's activities. The security implementation into organization itself is although for organization itself process very painful, longterm and relatively expensive.

Very often it comes to managers that the investment is paid uselessly and it would have been possible to use the resources, both financial and human, in better way contributing to success of the firm. This investment has in certain rate character of assurance – if nothing happens the investment is useless, but when "something" – respectively anything happens, then it is literally past payment.

For the security implementation into organization itself it is necessary knowledge and skills, which are not at common availability on IS/ICT market. This is why are basic mechanisms and customs saved into international standards (know-how), which were elaborated with participation of experts from many countries of the world – let's do not re-invent, what has been already invented. But for application of even the best standards it is necessary to approach in creative way, not mechanistic way, and it is necessary to be able to customize them on particular conditions, in which we want them to apply. Standards have world wide validity, but specifics of particular countries and cultures must be reflected by local experts. With this they not only confirm validity of international standards, but thoughts contained in them more over pays interest in bigger effects for the target organization.

6 Conclusion

Concept of integrated management systems represents complex approach to organizational management, in which are harmonized all parts of IMS with the management process as a whole. Implementation IMS into organization brings together several particular effects, which influence especially specific areas of IMS. The most emphasized ones are:

- increase in ability to compete on market thanks to quality management system implementation,
- presentation of firm in form of thoughtful behaviour to life environment in the moment of environmental management system implementation,
- personal assets securization and declaration to keeping basic human rights and freedoms by implementation of occupational health and safety at work management system,
- preservation of IS/ICT investments in implementation IS/ICT security management system.

Except of the abovementioned points, the first common effect is the possibility of executing integration in some internal activities for all parts of IMS – especially their audit and quality assurance of individual IMS parts. It is possible to combine and integrate parts of quality

management audit with IS/ICT security audit and alike integrate audit examination in area of occupational health and safety management with procedures of environmental audit.

For implementation and using IMS in organization are necessary knowledge and skills, which are not at common availability on IS/ICT market. The basic generalized mechanisms, customs and procedures are incorporated into international standards, which represent in effect world wide know-how, which has been elaborated with assistance of experts from many countries of the world. Even for management in this area pays – do not invent, what has been already invented. With using international standards we enable to transfer wide potential hidden in them into common praxis even with workers, which are experts in these areas. But attention – to application of even the best standards it is necessary to approach in creative way not in mechanistic way and it is necessary to customize them to particular conditions, in which we want to apply. Standards have world wide validity, but specifics of particular countries and cultures must be reflected by local experts. With this they not only confirm validity of international standards, but thoughts contained in them more over pays interest in bigger effects for the target organization. Of the biggest effect for the organization is the evidence, that their workers will perform the right things right.

References

Doucek, P. (2004). Global society and IS/ICT Security, In: *National and Regional Economics*, Technical University Košice.

Doucek, P. (2004). IS/ICT Security – Auditing and Control, In: *Management, Knowledge and EU – Proceedings of the 23th International Scientific Conference on Organizational Science Development*, Portoroz, Slovenia, March 24-26, 2004, Faculty of Orgamnizational Science, University of Maribor.

Nedoma, J., Nedomová, L. (2002). Standardizované systémy rízení. 1. vyd., Jihlava : Vyšší odborná škola Jihlava. (Standardised Management Systems)

Nedomová, L. (2001). Kap. B 5.6. Delat správne správné veci (Environmentální systémy rízení z jiného pohledu. In: *Podnik a životní prostredí*, Edited by Jonáš, F., Rohon, P., Suchardovová, D., Praha, Raabe. (Chapter B 5.6. Doing the rights things right (Environmental management systems from other view. In: *Business organization and life Environment*)

Sources

ČSN 36 9786 – ČSN/ISO/IEC TR 13335 1-5 Informační technologie – Smernice pro rízení bezpečnosti IT

ČSN 36 9789 – ČSN/ISO/IEC 15408 1-3 Informační technologie – Smernice pro rízení bezpečnosti IT

ČSN 36 9790 - ČSN/ISO/IEC 17799 – Informační technologie – Soubor postupu pro rízení informační bezpečnosti

ČSN EN ISO 9001 : 2000 Systémy managementu jakosti požadavky

ČSN EN ISO14001: 1997 Systémy environmentálního managementu - Specifikace s návodem pro její použití

ISO/IEC 15408-1-3 Information technology, Security techniques, Evaluation criteria for IT security

ISO/IEC 17799 - Information technology – Security techniques – Code of practice for information security management

ISO/IEC 18044 - Information technology – Security techniques – Information security incident management

ISO/IEC TR 13335-1-5 Information technology – Security techniques – Management of information and communications technology security – all parts

ISO/IEC TR 19791 - Information technology – Security techniques – Security assessment for operational systems

Petr Doucek has graduated at the Faculty of Management at the University of Economics, Prague in Mathematical Methods in Economy in 1984. Since 1997 is he associate professor for information management. Since 1990 he has been working as a member of the Department of System Analysis at the Faculty of Informatics and Statistics at the University of Economics, Prague. His main topics in research and development work focus on information management, IS/ICT security management, project management and impacts of information society building on human. He is author and co-author of seven monographies, 15 textbooks for students and more than 100 articles in proceeding books of international conferences, congresses and in reviewed international journals. He took part at more than 30 information system improvement projects into Czech as well as into international companies. Since 2002 is he representant of Czech Republic in ISO/IEC JTC1 SC27 – Subcommittee for Information Technology Security.

Lea Nedomová has graduated at the Natural Science Faculty at the Charles University, Prague in Pedagogy of Chemistry and Biology in 1992. Since 1996 she is assistant professor and secretary executive of Department of System Analysis at the Faculty of Informatics and Statistics at the University of Economics, Prague. Her main topics in research and development include system approach to global development and sustainable development, relation of quality management, environmental management and sustainability, and using information in social systems. Her publications include several monografies and dozens of contributions to conferences and reviewed journals.

Jan Klas has graduated at the Faculty of Informatics and Statistics at the University of Economics, Prague, with major in Information Management and minor in Accounting and Financial Management in 2001. He is PhD student of Informatics and since 2005 regular member of the Department of System Analysis at the Faculty of Informatics and Statistics at the University of Economics, Prague. His research work is oriented on areas of information management, virtual organization and social systems. Practical experiences include project management and IS/ICT systems development. He is author of about 20 contributions to international conferences or congresses and articles published in reviewed journals.