INFORMATION SECURITY ASPECT OF OPERATIONAL RISK MANAGEMENT

Janusz ZAWIŁA-NIEDŹWIECKI*, Maciej BYCZKOWSKI**

*Faculty of Management
Warsaw University of Technology, ul. Narbutta 85, 02-524 Warsaw
e-mail: j.zawila-niedzwiecki@wz.pw.edu.pl

**European Network Security Institute
ul. Jana Pawła II 34, 00-141 Warsaw
e-mail: maciej.byczkowski@ensi.net

Abstract: Improving organization means on the one hand searching for adequate product (service) matched to the market, on the other hand shaping the ability to react on risks caused by that activity. The second should consist of identifying and estimating types of risk, and consequently creating solutions securing from possible forms of it's realization (disturbances), following rules of rational choice of security measures as seen in their relation to costs and effectiveness. Activities of creating the security measures should be organized as constantly developing and perfecting and as such they need formal place in organizational structure and rules of management

Key words: operational risk, risk management, information security, information security management, IT security.

1 Operational risk

1.1 Operational risk management

Concept of operational risk, first as a definition and, next, as a full classification, appeared for the first time in documentation of Basel Committee[1] in the middle of 1990's. Although in its English form operational risk management is unfortunately similar to operational management of risk, the term became gradually more and more popular outside the banking industry and, recently, even outside the finance sector.

According to Basel Committee "operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." [1]. "The definition includes legal risk (i.e. the risk of loss resulting from failure to comply with laws, ethical standards and contractual obligations) but excludes strategic and reputational risk." [2].

An important matter seems to be the observation concerning universal character of the Basel Committee's concept from the point of view of other branches of economy. It can be safely stated that operational risk is the risk of sufficiently efficient functioning of an organization, characterized by the same regularities in case of financial institutions, production plants, trade companies or public administration.

Risk, as a characteristic of activity, is subject to influence of conscious management, which means both possibility and professional obligation to manage it in such a way to identify, analyze and estimate it. On basis of this knowledge, its level and signs should be influenced. Classic model of such approach to management is presented in Fig. 1.

Such a complex risk management should lead to a situation, in which the organization (management) is aware of risk and its magnitude. Awareness means, that risk has been identified, researched from the point of view of its causes, way of realization and scope of possible effects.

The most important stages of risk management are: risk identification, analysis and measurement (assessment). Until this happens, it is hard to speak concretely of risk, because risk-limiting or security actions cannot yet be taken. In general, it can be stated that, without knowing the risk, one deals with a threat viewed, above all, as: unawareness, recklessness, negligence.

When appropriate diligence of activity is maintained, there is no speaking of unclear threat. On the contrary, the risk is referred to as probability of given result or probability distribution of an imaginable set of results. This is described by the most general risk equation: R = P x I, where R refers to risk, P to probability of an event, I to the influence of the event on the organizational activity (size of losses).

[1] Basel Committee on Banking Supervision "Operational Risk Management", IX.1998.

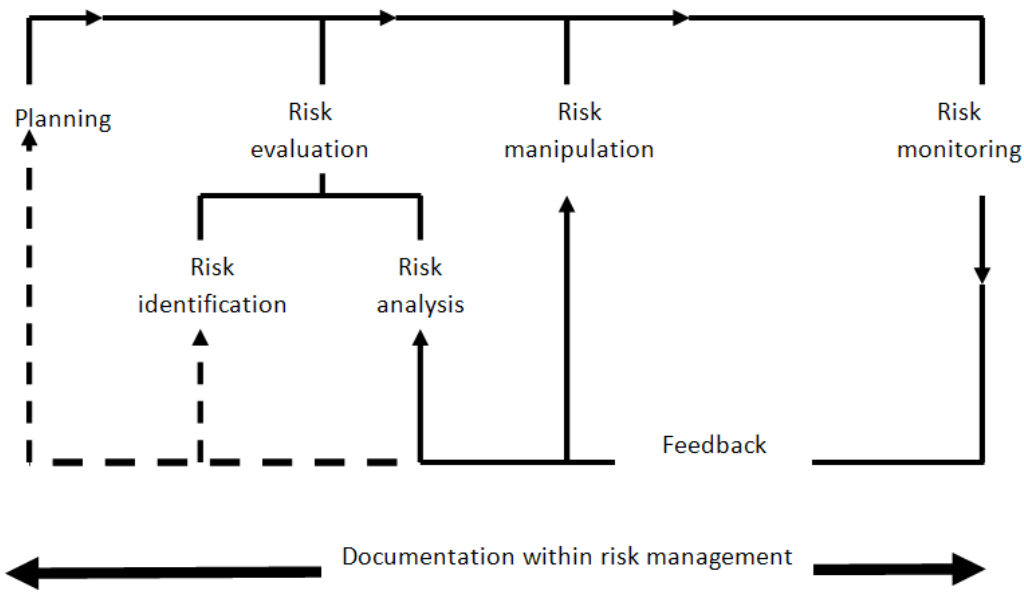


Figure1. Structure of risk management process
(source: [6])

In the operational risk management it is not a risk of single, critical event that matters, but the general map of risk composed of all possible critical events. This enables us to determine total risk, risk of especially probable events or risk of especially severe events. The above mentioned equation points to two fundamental risk factors, which, in the course of analysis, allow us to classify particular possible critical events according to their importance for the appropriate functioning of the organization. Subsequently, intensive actions can be carried out towards those critical events, which were found most important during the analysis. This is shown in Fig. 2.

Reaction to critical events, viewed as signs of risk, may refer to causes of these events (prevention as ex-ante activity) or to their results (therapy as ex-post activity). The first type of activity is referred to as ensuring operational security, the second one as ensuring business continuity. Reactions of both types base on analysis of risk, its causes and effects, but also on the analysis of core organizational activity – the one that is characterized by the given sign of risk. In reality, risk reveals itself through phenomena of a given character, but the final influence on organization is only possible, when such phenomenon encounters organizational vulnerability concerning one or a few organizational processes, either in the sense of organizational imperfectness of such a process, or weakness with regard to choice of resources used by the process. Therefore, risk analysis consists in determination and evaluation of:

- processes which decide about realization of organizational tasks,
- set of disrupting phenomena and probability of their occurrence,
- resources vulnerability, in the sense of magnitude of disruptive phenomenon potential influence on organizational activity.

A desirable situation is to possess sufficiently reliable statistical data, which describe probability distribution of disruptive events. In reality, however, this happens with regard to not so many types of events, though i.e. Basel Committee has recommended, and Polish governance organs including Polish Financial Supervision Authority (before 1.01. 2008 Commission for Banking Supervision) instructed to gather such statistical data within framework of systematic risk analysis. In case such statistical data is unavailable, what remains is to perform evaluation based on risk factors assessment. It is, nevertheless, necessary to assume that an entity with high organizational culture, independently from governance bodies' requirements, will gather and analyze adequate statistical data, referring to the organization and its activity, out of its own belief.

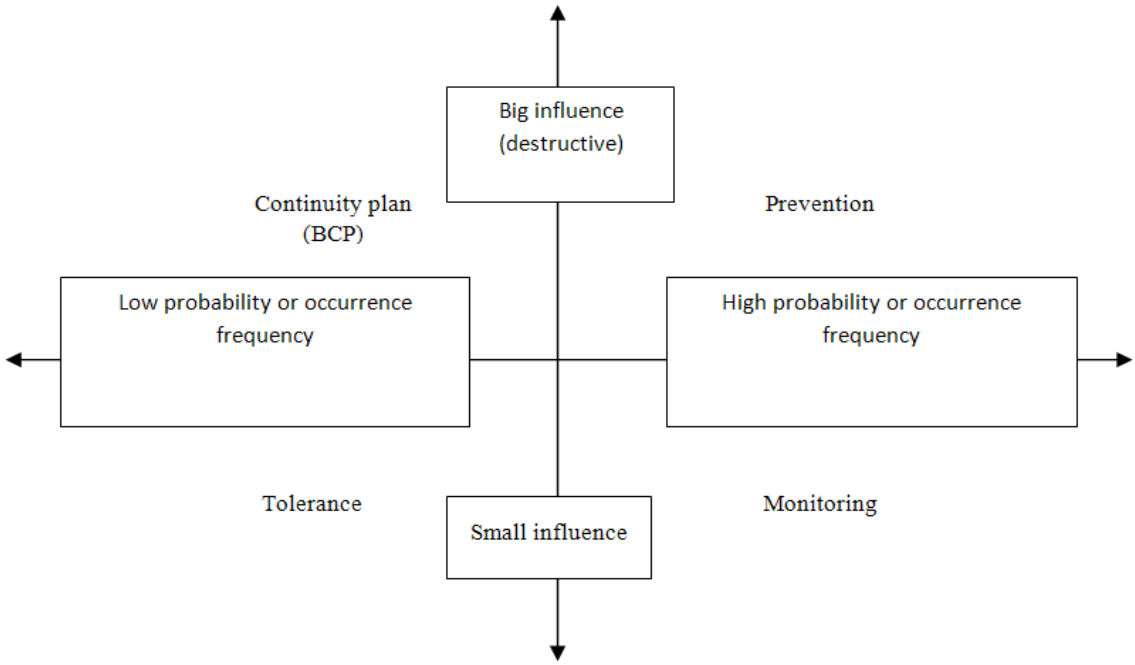


Figure 2. Model approach to threats
(source: [16])

Currently, there exists no final classification or convincing-enough interpretation of types of operational risk. At present, it is only possible to suggest directions for such classification, which could consist in presenting types of risk in three different orders:

- from the point of view of causes of critical events,
- from the point of view of mechanism of their realization,
- from the point of view of critical events results.

An approach towards classification of operational risk from the point of view of its causes could be the well known and often quoted in literature proposition [10]: fraud risk, lack of reconstruction plans after a catastrophe, regulatory risk, risk of losing reputation, administrative risk. However, this classification is relatively superficial because it lacks clear explanation for the chosen criteria of division.

This requirement is, on the other hand, fulfilled by classification shown in Table 1. It is based on the observation, that risk realization is a result of given type of threat's interference with an organizational vulnerability, which reflects organizational actions inefficiency. Therefore, organization and its threat vulnerability was treated with the use of process approach, which includes interpreting management model as goal realization through a cycle of managerial activities based on use of basic types of resources.

The classification described below does not meet such rigorous assumptions concerning ordering criteria. However, it is the most commonly quoted one because it is recommended in Basel II documentation and EU regulations as well as Polish Banking law. It consists in dividing risk into categories: internal fraud, external fraud, staff policy and occupational safety, clients, products and business policy, damage to physical assets, disruption of activity and system failures, carrying out transactions, process management [8].

This classification, as an approach of experienced professionals to order the list of well-known and repetitive critical events, is also used outside the banking sector. However, when it comes to designing security and business continuity solutions, this classification causes some problems. These problems refer to lack of sufficient precision in distinguishing between particular categories and ambiguous ascribing of responsibility. Therefore, when designing risk management solutions, most commonly a simple division is used, which encompasses:

- management of physical and technical security,
- management of personal security,
- management of information and IT systems security,
- business continuity management.

Table 1. Classification of types of operational risk
(source: [16])

<table>
<tr><td colspan="3"></td><td colspan="6">↑ Vulnerabilities ↑</td></tr>
<tr><td colspan="3"></td><td colspan="6">Organizational efficiency</td></tr>
<tr><td rowspan="11">↓ Threats ↓</td><td rowspan="3">Environment</td><td colspan="7">Risk of natural disasters</td></tr>
<tr><td colspan="7">Risk of terrorism</td></tr>
<tr><td colspan="7">Risk of external disruption of functional working environment (i.e. lack of access to headquarters)</td></tr>
<tr><td rowspan="3">Core processes</td><td colspan="7">Risk of physical working environment disruption (i.e. too high temperature)</td></tr>
<tr><td colspan="7">Risk of internal disruption of functional working environment (i.e. strike, accident)</td></tr>
<tr><td colspan="7">Risk of disruption of technical working environment (i.e. A/C malfunction)
including
Risk of disruption of IT working environment (i.e. computer malfunction)</td></tr>
<tr><td rowspan="7">Supporting processes</td><td rowspan="7">Areas of risk realization (expression of resources security and organization)</td><td colspan="6">Ideal organization postulates (expression of management goals)</td></tr>
<tr><td></td><td>Effective</td><td>Efficient (organizationally optimal)</td><td>Rational (cost-optimal)</td><td>Safe</td><td>Repetitive</td></tr>
<tr><td>Human resources</td><td>Risk due to lack of competence</td><td colspan="2">Lack of staff reserves risk</td><td>Risk of staff fluctuation</td><td>Risk of relative interpretation
Risk of ill will</td><td>Risk of routine (fossilization)</td></tr>
<tr><td>Material resources</td><td>Risk due to lack of functionality</td><td colspan="3">Risk due to lack of material reserves</td><td>Risk of side-effects</td><td>Risk of wearing-out</td></tr>
<tr><td>Financial resources</td><td>Risk due to unsuitable expenditures</td><td colspan="3">Risk of excessive expenditure</td><td colspan="2">Risk of running out of resources</td></tr>
<tr><td>Information resources</td><td>Risk due to lack of full information</td><td colspan="3">Risk of not keeping up with development</td><td>Risk of inaccessibility</td><td>Risk of distortion</td></tr>
<tr><td>Management processes</td><td>Organization</td><td>Risk of an incident (malfunction)</td><td colspan="3">Risk due to lack of organizational potential</td><td>Risk of security superiority over efficiency</td><td>Risk of deficiencies</td></tr>
</table>

1.2 Risk analysis

The most common approach is so called BIA (business impact analysis), based on identification of core processes and their particularly critical elements as well as factors, which may negatively exploit this criticality. Such a primary analysis is then described in detail through assessment of the identified risk. An exemplary assessment is provided by TSM-ORA method (total security management – operational risk assessment) [17].

First stage of analysis in this method consists of:

- determination of system boundaries, within which its resources are located,
- description of environment, in which the system operates (both physical as well as legal and organizational one),
- definition of assets.

It consists in determining goals and business system functions, which require ensuring resource availability; next, in determining system processes aimed at realization of system goals, and, finally, determining resources (also intangible), which enable that. Assets should be assigned values, which would determine their importance in the light of system goals. These values should relate to costs of obtaining and maintaining the assets.

Second stage is the identification of threats. Their analysis consists in determining which of them actually concern the analyzed system and what is the probability of their occurrence. This probability may depend on the type and value of business system asstes, which are exposed to particular threats. Evaluation of such resource vulnerability may be carried out in two ways. First of them is to create a list of system weaknesses, which could be used by potential sources of threats, and to assess the easiness of their use. This technique

is difficult in the sense that business weaknesses are most often observed after the vulnerability has been used and caused disruption. A reliable-enough evaluation is possible in this case only on the basis of gathered statistics of incidents, which, in reality, are still very rare. The second method is to start from identified threats and evaluate, how vulnerable to them the particular assets are. When it comes to system interaction with threat, as a result of use of vulnerability, we speak of disruption.

Crowning of the risk analysis process is elaboration of map of potential disruptions, which comes into being after combining analysis with assessment of two factors (see Fig. 2): probability of the disruption and influence of this disruption on the business system.

One consequence of risk analysis is that, subsequently, works on ensuring security and business continuity are being undertaken. Those are achieved through solutions for manipulating and monitoring signs of risk.

1.3 Codes of best practices

Such codes of best practices are [14]:

- COSO-ERM, Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management,
- FERMA, Federation of European Risk Management Associations,
- POLRISK, Polish Risk Management Association,
- MiFID, Market in Financial Instruments Directive,
- M recommendation of Polish Banking Supervision Inspectorate,
- ISO 27005 standard,
- AS/NZS 4360 standard.

Risk management maturity may be evaluated with the use of model suggested for banking industry with regard to financial risks (BBA model [3]). A sufficient analogy exists here concerning organizational and methodical rules.

2 Organizational security

2.1 Security viewed as value

In the context of operational risk management, security is a certain state of social and subjective reality, limited to a single organization or branch of similar organizations. From the general society point of view, which is characteristic for crisis management, it appears to be, above all, a value. “On one hand it is a certain social, civilization, cultural, economic and ecologic value, etc. – on the other, however – it is a hard-to-overrate existential, moral and spiritual value” [15].

In accordance with Maslow’s research [11], feeling of security is the second need among fundamental human needs. Therefore, it is right to say that “goal of crisis situation management is not just fastest possible return to normality. The essence of this type of management is to force an organization to become aware of moral and social responsibility with regard to internal and external stakeholders.” [13]. Creating such a awareness, both in solely professional (organizational culture) as well as social and moral dimension, is currently a great challenge in the field of management. It is defined as corporate social responsibility (main idea of Forum in Davos, since 1980’s).

2.2 Ensuring security viewed as risk manipulation

Security issues are realized through solutions, which mainly aim at prevention, consisting in observation of threat factors, monitoring of characteristic and typical symptoms of their activation and prevention of their interaction with organizational business system and organization environment. If these actions fail and the organizational activity is disrupted, it means it is the time for planned and organized reconstructive activity, which should determine the acceptable ability to maintain business continuity.

In design of security solutions, the following general rules, which are mainly referred to people as the main source and object of threat, are used [16]:

- rule of authorized access – each employee has undergone a training in principles of security and protection and meets the job and information access criteria (official secrets),
- rule of necessary privileges – each employee has only these job and information access rights, which are necessary for him to carry out his tasks,
- rule of necessary knowledge – each employee has at least the knowledge about the job, to which he has access, that is necessary to carry out his tasks,
- rule of necessary services – organization provides only those services which are demanded by client,
- rule of security measures – each security mechanism must be protected by another (similar) one,

and in special cases additional (third), independent security measure may be used,
- rule of collective awareness – all employees should be aware of the necessity to protect organizational resources and actively participate in this process,
- rule of individual responsibility – particular persons are responsible for particular elements' security,
- rule of necessary presence – the right to be present at given places is granted only to authorized persons,
- rule of constant readiness – organization is prepared for each and every threat; temporary switching-off of security mechanisms is unacceptable,
- rule of weakest link – level of security is determined by the weakest (least secured) element,
- rule of completeness – effective security measure is only possible when a complex approach is taken, which includes all levels and parts of the general working process,
- rule of evolution – each organization must constantly adapt its internal mechanisms to changing external conditions,
- rule of suitability – mechanisms used must be suitable to the situation,
- rule of acceptable balance – security measures used cannot exceed the level of acceptance (cost measures with regard to outlays, effects and potential losses are especially advised here).

2.3 Areas of ensuring organizational security

Ensuring organizational security refers to particular types of resources. Therefore, personal, physical, technical, financial, information and IT security are distinguished. As can easily be seen, particular categories remain in tight relationship to one another and, partially, even overlap. One speaks of: physical security of people, security of personal data, financial instruments' physical security etc.

Ensuring physical and technical security is derived from the following key rationales:
- need for precise definition of organizational location boundaries and spheres of provision of particular functions and services for clients, as well as through and for the organization employees,
- need for imagining and defining potential threats and their possible realization scenarios as disruptions of normal organizational work,
- need for organization of processes concerning organizational functions, organization of ensuring physical security as well as choosing and applying security measures, including technical ones.

Employment of good practices with regard to this issue consists in elaboration of:
- division (classification) of security zones,
- rules for choosing security solutions,
- security rules for particular zones,
- rules of access authorization,
- rules of security control,
- rules for choosing and verifying security employees.

Ensuring personal security, on the other hand, is derived from the following key rationales:
- need for choosing and employing people who are characterized by high level of morale and responsibility (so called "righteousness rule"),
- requirement concerning adequateness of employees' professional sills with their tasks and potential ability to adapt to changing requirements, which may result from organizational and business development of the organization or competitive market development (so called "competence rule").

Employment of good practices with regard to this issue consists in elaboration of:
- employee ethics code,
- rules of employees selection and verification,
- rules of entering and leaving the organization,
- rules of determining individual and team roles as well as designing workplaces,
- rules of delegating tasks,
- rules of remuneration and motivation,
- rules of staff reviews,
- rules of determining individual career paths,
- rules of promoting employees,
- rules of systematic employee training,
- rules of protecting secrets of company, clients, etc.

As far as ensuring information security is concerned, it is derived from the following key rationale:
- ensuring that information is made accessible only to authorized persons (so called confidentiality rule),
- ensuring total precision and completeness of information and methods of processing information (so called "integrity rule"),
- ensuring that authorized persons have access to information and related assets only when there is such a need (accessibility rule).

Three levels of content-related information security management are distinguished:

- information security policy – determination of security requirements at the level of whole organization and with regard to all information groups, systems and solutions, which are used to process these information (including storing and transportation),
- information group – specification of security requirements for information groups, mainly distinguished as an autonomous class of information used for specific problems, processed in a given functional department (i.e. financial information, staff information, client information, etc.), but also, in some cases, covered by separate legal regulation i.e.: classified information, personal data information,
- processing system – fulfillment of security requirements both by traditional and IT systems, which process certain groups of information for particular categories of users.

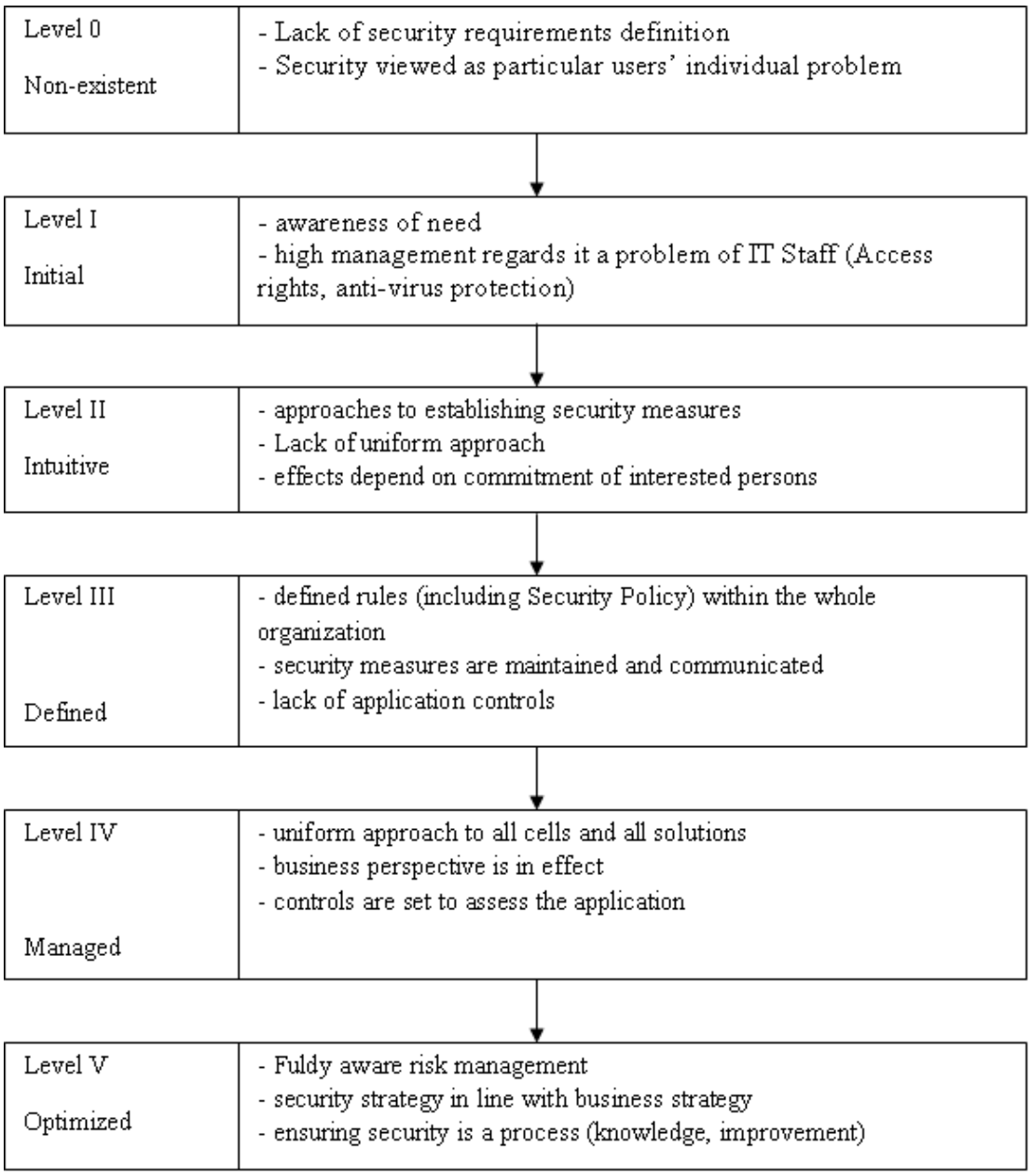


Figure 3. Information security management maturity levels
(source: [7])

2.4 Management of ensuring security

Security management in an organization is conducted differently, depending on the area it concerns. And so, physical security management, but also occupational hygiene and safety, is institutionalized (partly defined by general law i.e. concerning occupational hygiene and safety, or industry law, i.e. banking) and takes form of separate workstations/cells. On the other hand, personal security management in the area of "hard approach to HR" is also institutionalized, whereas in case of "soft approach to HR" it has a character of a certain organizational activity policy towards employees and of researching its effectiveness in relation to employee attitudes towards tasks and the employer. Furthermore, information security management consists in appointing specific roles to employees, who, at the same time, fulfill other tasks within the organization. Especially with regard to IT security it is connected with the necessity of constant development of professional knowledge from the field of IT, which is dynamically changing. Similarly, the security requirements change.

In case of security ensuring activities there is a general rule of separating tasks concerning determination of security standards/requirements/rules and controlling their fulfillment/abidance from tasks concerning their implementation/appliance. This is achieved through delegating them to separate persons/organizational cells.

2.5 Codes of best practices

- Act on Protection of Persons and Property (consolidated text.: Journal of Laws 2005, no. 145, pos. 1221),
- Banking Act,
- Personal Data Protection Act,
- European Committee resolution no. 2001/246/EC of 19 March 2001 (reviewed on 19.11.2001),
- ISO/IEC 27002:2007.

Fulfillment of the information security ensuring rules described so far is a basis for evaluation of security management maturity. A model for such evaluation was proposed by Information Systems Audit and Control Association (ISACA).

3 Information security

3.1 Information security management

Ensuring security of the processed information in an organization has to consist in providing complex solutions to the problems of information and information security management, as well as in implementation and development of security measures (organizational and technical). The primary goal is the protection of the interest of a given organization (business security) and minimizing risk of legal consequences on the ground of lack of security or improper activities towards information, the protection of which is required by law. Therefore, a complex solution must encompass both business and legal aspects of information security.

Such a complex approach recommended by various standards is ISMS (Information Security Management System ISO 27001, in Poland: PN-ISO/IEC 27001:2007). "Information Security Management System is a part of the total management system, based on the approach which results from business risk, referring to establishing, implementing, using, monitoring maintaining and improving information security". ISMS has an interdisciplinary character, combining different disciplines including: information technology, law, organization and management. Introduction of this type of system is important because it creates a stable company image of being worth the trust of a wide group of stakeholders. Standards do not say precisely how to build the management system. Therefore, in practice, it is possible to base on expert solutions. According to TISM (Total Information Security Management – ENSI methodology) methodology, organization of ensuring information security, with regard to information that is processed within the organization, consists in establishing rules of information management at three levels: Information Security Policy, Information Groups and Processing Systems (source: [4, 5]).

At the level of information security policy basic rules for protection of information within organization are established. At the level of information group specific requirements towards protection for given group of information are established. At the level of processing system the fulfillment of requirements of the higher levels by a processing system, containing given group of information, is assessed.

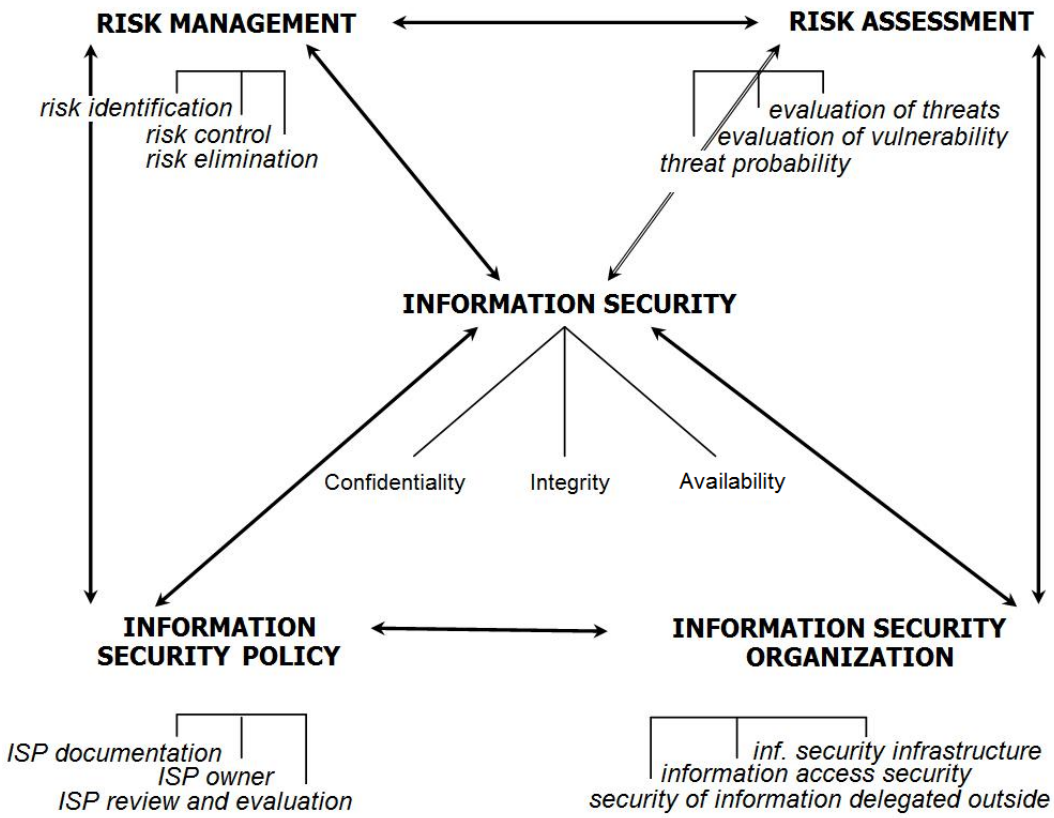


Figure 4. Aspects of information security management
(source: [4])

Information security concept is based on three pillars:

- existence of a suitable organizational structure with regard to information security management,
- information classification – division into limited information (company secrets, to be used within company) and public information (publicly available),

setting appropriate processing (zones) and storing places (IT system, paper archives).

3.2 Structure of information security management

Through elaboration of information security policy and appropriate internal regulations of an organization a specific information and information security management structure is formed. It consists, in accordance with TISM, in determination of proper managerial and controlling roles, which, in line with the "rule of two" (separate management of information processing and establishment of security guidelines and control of compliance with them) are grouped in two functional departments: managerial (administrative) and control (security), and refer to three levels of information security management presented above.

At the level of information security policy the following roles are defined: Information Manager (IM – most often a member of the highest management) and Plenipotentiary for Protection of Information (PPI). At the level of information group, the roles of: Information Resource Manager (IRM – most often the head of organizational department) and Information Security Administrator (ISA), are defined. At the level of information processing the roles are: System Administrator (SA), System Security Administrator (SSA), for big organizations Chief Security Systems Administrator (CSSA). The primary role in information security management is played by PPI. All the employees of both departments, who fulfill the mentioned roles are subordinate to him. Control (security) department is responsible for supervision and control of information security at each of the three levels. The roles cannot be combined between the departments. However, one person can fulfill the role of ISA for a couple of information groups. Also, one person can be the SSA for a couple of processing systems.

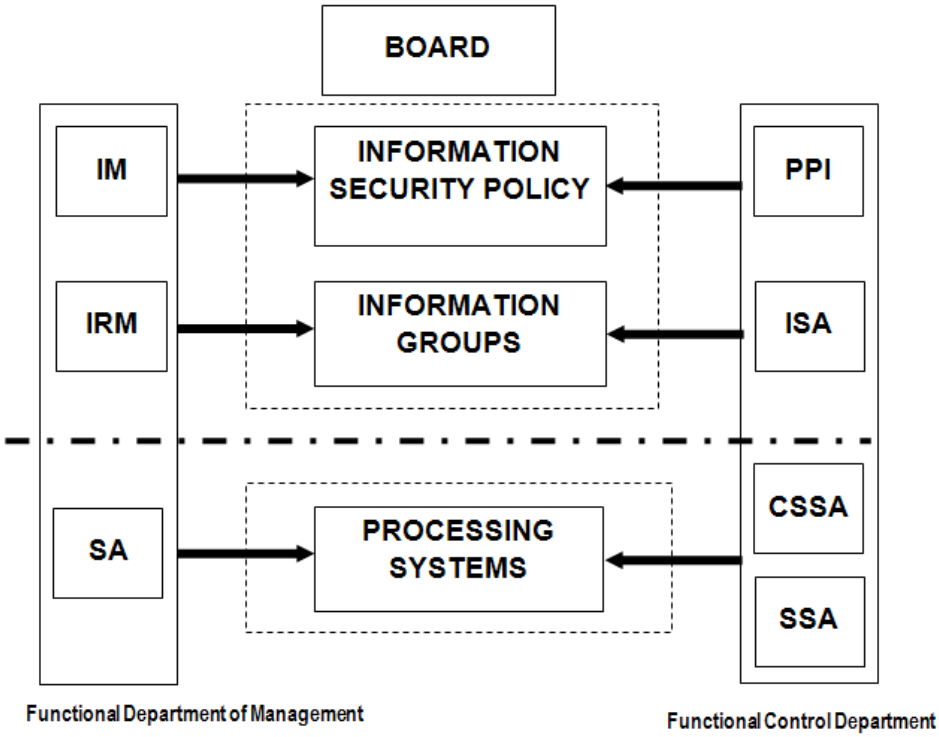


Figure 5. Structure of information management and information security management *(source:[4,5])*

3.3 Information security management processes

Processes of information security management encompass the management of all information resources (including resources aggregated in IT systems) and their use on three hierarchical decision levels: strategic, tactical and operational.

At the strategic level a general information security policy is conducted, with regard to identified, defined and analyzed risk and fundamental expectations towards level of information security and with regard to model tasks and solutions, which result from these expectations. Therefore, the highest management is involved in the decision processes at this level. The highest management determines fundamental information security criteria (derived from normative criteria and to be realized on the basis of identified attributes of information).

At tactical level information security standards and rules for control of their execution within the IT solutions and products, which are used, are established. Also, standards for compliance in practice with proper use of those solutions and products are created (in accordance with the pre-determined levels of security: standard, increased or special).

These decision processes involve mainly the management of departments responsible for general, physical, technical, personal and information security as well as information technology.

At the operational level, information security administration is carried out from the viewpoint of full employment of security standards and solving disruptive situations, which result from breaking these standards (intentional or accidental).

In the information security management organization it is assumed, that basic rules for creation of total security and information security management structures are:

- complete separation of management and controlling functions from executive functions,
- preventing misconduct and maximal limitation of mistakes made by individuals within the area of one-man responsibility,
- ensuring independence and unbiased character of individuals who carry out security audit, having guaranteed that the company secrets will be kept.

All the security processes, security solutions and organization of ensuring security must stay in accordance with the above mentioned rules.

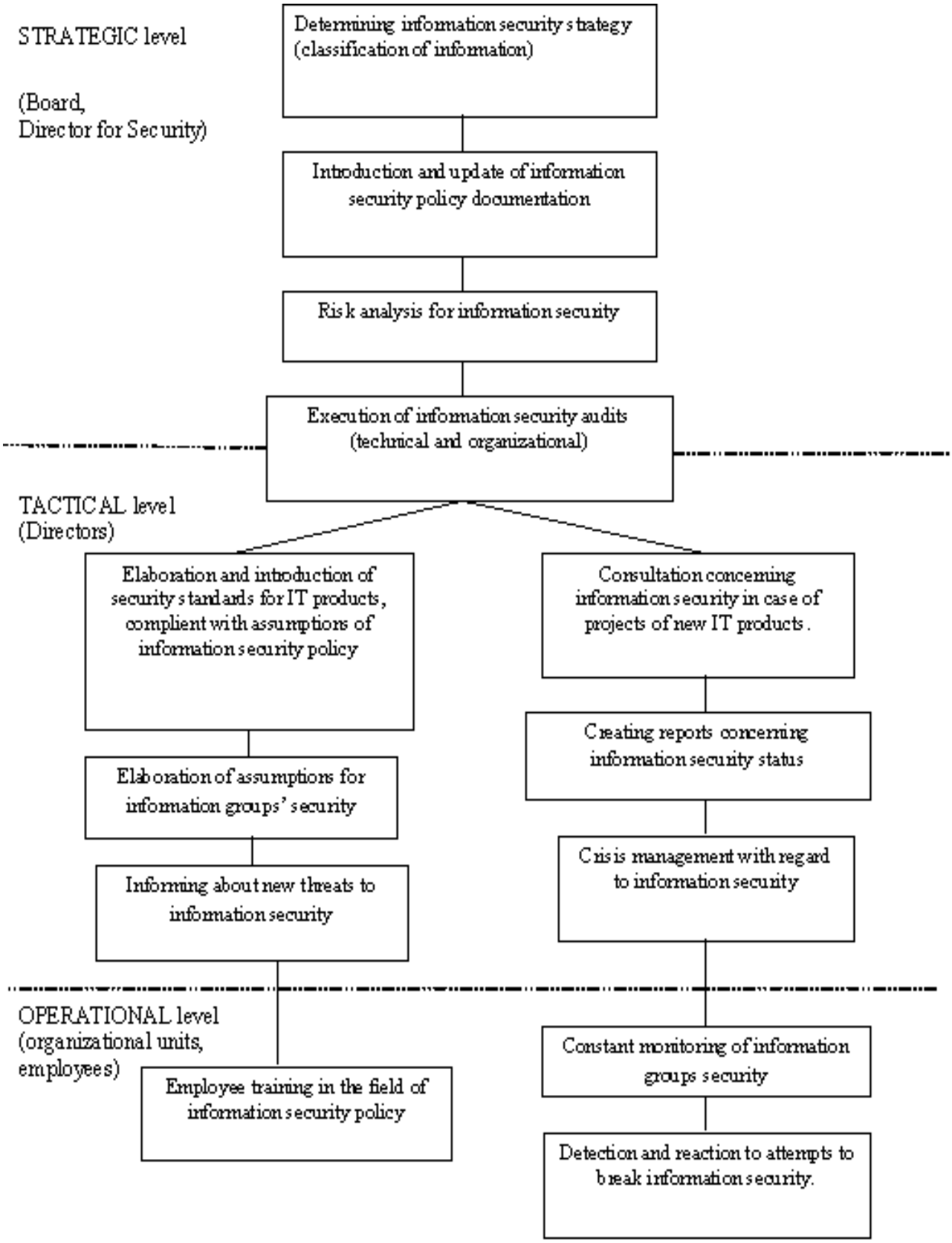
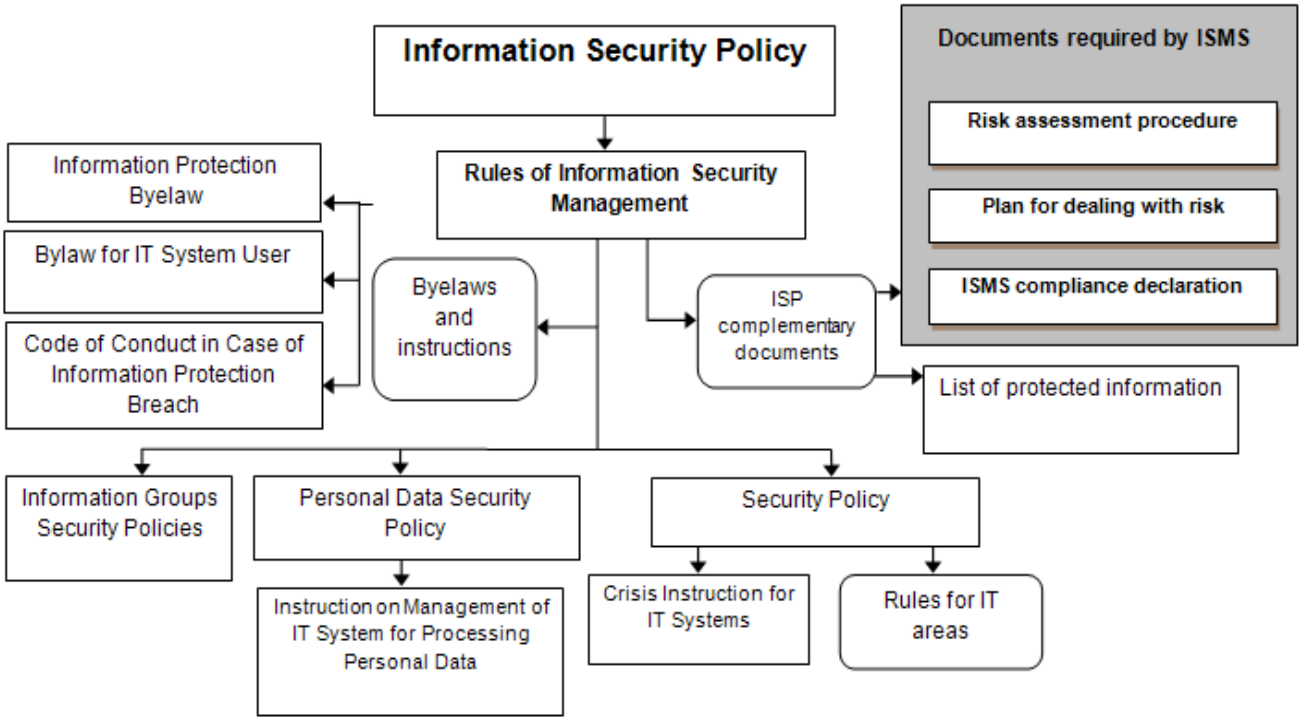


Figure 6. Processes of information security management
(source: [16])



Fiure. 7. Map of Information Security Policy documentation
(source: [5])

3.4 Information security policy documentation

Rules for protection of information should be contained in information security policy – set of documents aimed at certain users (managers from both departments and all other users of information), which consists of:

- Information Security Policy – main document,
- Rules of Information Security Management,
- Regulations, including:
  - Information protection byelaw,
  - IT system user's byelaw,
- Information Groups Security Policy, including
  - Policy for Personal Data Security,
- IT system security policy, including:
  - Rules for IT areas,
  - System procedures and configuration standards,
- Instructions, including:
  - instruction on conduct in case of breach of information protection,
  - instruction on management of IT system for processing personal data.

The Information Security Policy document defines:

- which information groups will be subject to protection (this means that, through formal internal management, groups of protected information are determined, including: company secrets, personal data and legally protected information, while all the other information will be regarded public),
- which systems will process protected information (broad understanding of processing system as both IT but also traditional, paper one),
- who and on ground of what rules will have access to protected information (information users – employees, persons from outside),
- who will be responsible for information security in the whole organization (Plenipotentiary for Information Security),
- who will be responsible for management of protected information groups (Information Resources Managers),
- who will be responsible for management of protected information groups security (Information Security Administrators),
- who will be responsible for security of information groups processing systems (System Security Administrators).

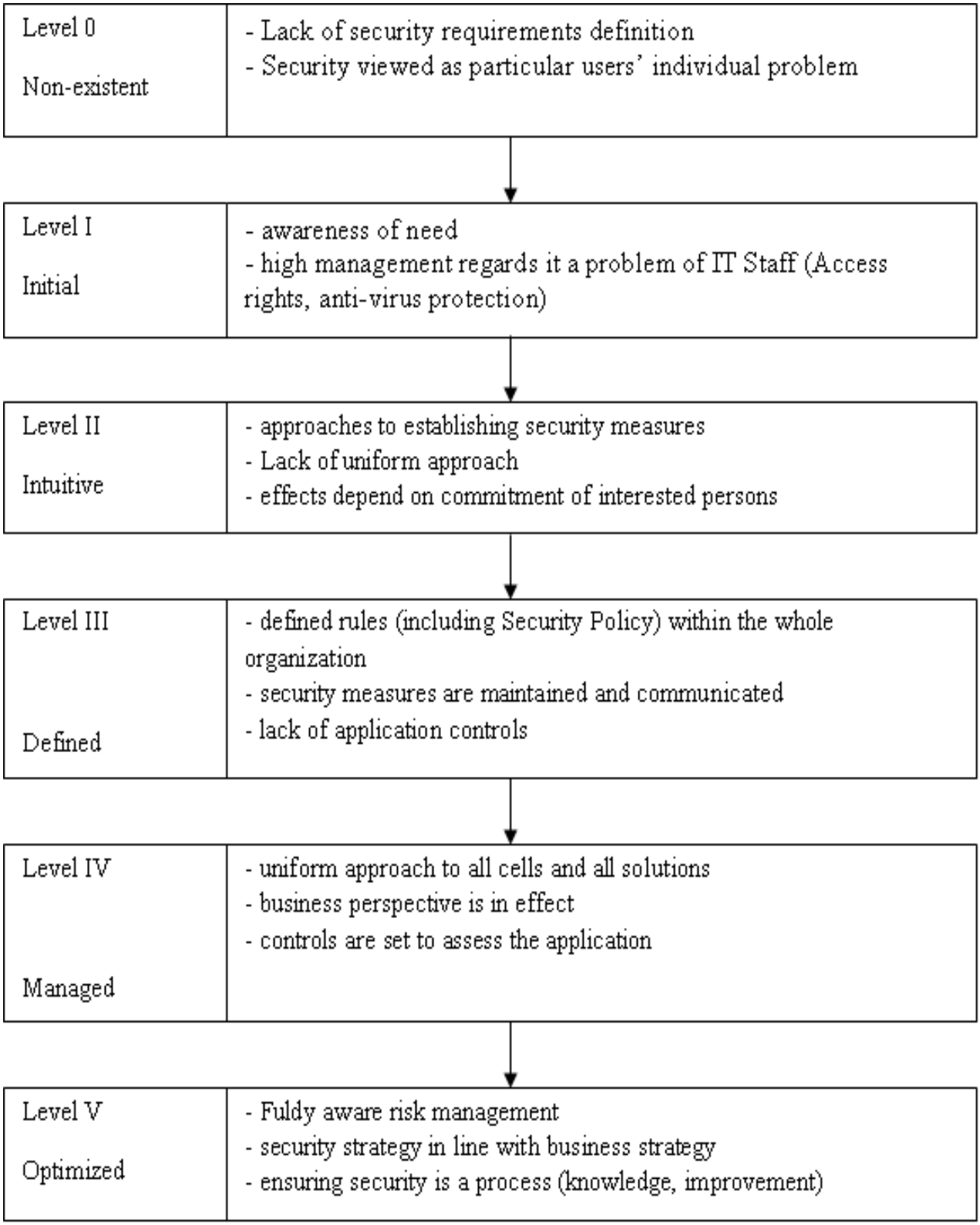


Figure 8. Information security management maturity levels
(source: [7])

Rules of information security management defined by Information Security Policy are applied for:

- all employees in the understanding of Labour Law, consultants, interns and other people, who have access to protected information,
- all existing, currently implemented or to-be-implemented IT and paper systems, in which protected information are or will be processed,
- all paper, magnetic or optical storage means, which contain or will contain protected information,
- all locations – structures and rooms, in which protected information will be processed.

"Rules of Information Security Management" document defines:

- goal and scope of management,
- general security rules,
- classification of information (limited, public),
- access to protected information,
- management of protected information processing,
- security requirements for information processing systems,
- rules on dealing with crisis situations,
- management of information groups users,
- information security management structure,
- rules for delegation of roles,
- rights and obligations for roles in controlling (security) department,
- rights and responsibilities for roles in administrative (management) department,
- reference to byelaws, procedures, instructions and standards defining information management.

Exemplary byelaws are: information protection byelaw, computer system user's byelaw.

Exemplary byelaws are important as they apply for all information users. They might be separate documents or one document, the model of which contains:

- definitions of basic concepts,
- scope of use of byelaw,
- division and ownership of processed information,
- list of protected information,
- general rules for using information and their protection,
- rules for protection of information in IT systems,
- rules for using Internet for protected information processing,
- rules for using information storage devices,
- rules for protected information processing on portable computers,
- rules for protection of rooms in which protected information are processed,
- rules of granting access to protected information, control of information protection, responsibility for breaking the rules,
- declarations of keeping information confidentiality.

Security policies for information groups result from legal requirements and define specific requirements concerning protection and processing of information from a given group (i.e. personal data, confidential information, stock-exchange information, etc.), requirements concerning access to a given group of protected information, as well as guidelines for creation of particular security instructions and procedures with regard to information groups.

IT system security policy describes specific security rules for such areas as: access control, cryptography, IT networks, servers, workstations, network services, business users' applications, portable computers, antivirus protection, monitoring and detection of security breaches and malfunctions, emergency plans and procedures for reconstruction of infrastructure, security audits and tests, new systems development and implementation.

Security rules for IT system areas also define the needs and guidelines for creation of particular procedures and security standards. In the stage of establishing systems they take form of security assumptions.

Standards are documents which describe configuration of particular elements of processing systems, such as: operation systems, databases, applications, telecommunication network, encryption and electronic signature.

Standards are established in order to ensure appropriately uniform level of security of protected information processing systems. Examples of standards are model configurations of server, e-mail or user's workstation.

4 IT systems security

With reference to strictly IT systems, in order to meet security requirements, standards such as ISO 12207, ISO 13355, ISO 15408, ISO 27000 series and codes

of best practices such as ITIL [19, 9] standard have to be used.

The established security solutions, that is: formal rules, management organization and their technical implementation (including IT) must, without exceptions, apply the rules of best practices named above, which were, out of necessity, very synthetically characterized in Fig. 8.

A properly constructed IT system should, regardless of form and character of information, fulfill three fundamental criteria:

- ensure information security,
- ensure security of providing services,
- ensure authenticity and accountability of data and subjects.

First criterion consists of the following elements:

- information confidentiality – which means that the information are only accessible for the authorized persons,
- information integrity – which means guaranteeing precision and completeness of information as well as methods of information processing,
- information availability – which means ensuring that authorized users have access to information and resources connected with them always when this is necessary.

Second criterion consists of the following elements:

- reliability of systems – which means the system may be always counted on, is user friendly and "fool proof",
- integrity of systems – precision of system and methods and ways of information processing used in this system,
- system availability – which means that authorized users are guaranteed access to system and its resources.

Third criterion consists of the following elements:

- Data indisputable – data which is stored in the system and accessed via the system is trustworthy and reliable,
- Indisputable of subjects – which refers to precision of system-using subject identification and confirmation of his authorization to use information gathered in the system,
- Settlement accounts of subjects – which refers to ensuring that authorized users do not have the ability to deny having accessed the system and the use of system resources is documented.

Meeting the so-far mentioned rules of ensuring information security is a basis for evaluation of security management maturity. A model for that was proposed by the IT auditors association ISACA.

Ensuring information security is a part of activity which constitutes a response to the identified operational risk factors.

Consequently, it is based on the rules characteristic for this more general issue, which draw significantly from the achievements of quality approach.

Simultaneously, ensuring information security and, in many aspects, IT security, consists in specific rules. An approach to signalize these rules was made in this work.

5 References

[1] Basel Committee on Banking Supervision -*Sound Practices for the Management and Supervision of Operational Risk*. 2003.

[2] Basel Committee on Banking Supervision - *International Convergence of Capital Measurement and Capital Standards*. 2006.

[3] BBA, ISDA, RMA - *Operational Risk: The Next Frontier.* British Bankers Association, London 1999.

[4] Byczkowski M., Zawiła-Niedźwiecki J. - *Zasady zarządzania bezpieczeństwem informacji w ujęciu metody TISM* [in] Zarządzanie rozwojem organizacji w społeczeństwie informacyjnym (Stabryła J. ed.). Studia i Prace Uniwersytetu Ekonomicznego w Krakowie, Kraków 2008, pp. 162-172.

[5] Byczkowski M. - *Metodyka TISM 2009*. ENSI, Warszawa 2009.

[6] Conrow E.H. - *Effective Risk Management. Some keys to success.* American Institute of Aeronautics and Astronautics Inc., Reston 2000.

[7] Forystek M. - *Audyt informatyczny*. Infoaudyt, Zgierz 2005.

[8] Główny Inspektorat Nadzoru Bankowego - *Rekomendacja M*. 2004.

[9] Hiles A. - *Service Level Agreements: Measuring Cost and Quality in Service Relationships*. Chapman & Hall, London 1993.

[10] Kendall R. - *Zarządzanie ryzykiem dla menedżerów. Praktyczne podejście do kontrolowania ryzyka*. Liber, Warszawa 2000.

[11] Maslow A.H. - *W stronę psychologii istnienia*. Rebis, Poznań 2004.

[12] MiFID - *Dyrektywa 2004/39/ EC, Rozporządzenie Komisji nr 1287/2006, Dyrektywa 2006/31/ EC, Dyrektywa 2006/73/ EC*. 2004-2006.

[13] Mitroff I.I., Pearson C.M. - *Zarządzanie sytuacją kryzysową*. Business Press, Warszawa 1998.

[14] Serewa M. - *Metodyka zarządzania ryzykiem organizacyjnym przez jednostki administracji publicznej*. Zarzadzanie Przedsiębiorstwem 2/2007.

[15] Szmyd J. - Bezpieczeństwo jako wartość [in] Zarządzanie bezpieczeństwem (ed. Tyrała P.), Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000, pp. 112-119.

[16] Zawiła-Niedźwiecki J. - *Ciągłość działania organizacji*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008.

[17] Zawiła-Niedźwiecki J., Soczko. M - Ryzyko operacyjne i jego szacowanie [in] Komputerowo zintegrowane zarządzanie (ed. Knosala R.), Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, Opole 2008, pp. 604-614.

[18] www.gloriamundi.org, 2009.

[19] www.ogc.gov.uk, 2009.