THE IMPORTANCE OF SECURITY POLICY FOR THE MINISTRY OF DEFENCE OF THE CZECH REPUBLIC

Author of the Essay: **Zdeněk Hais**

zdenek.hais@fsc-praha.cz

Author of the Presentation: **Tomáš Kubínek**

tomkubinek@volny.cz

F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a.s.
Vítkovická 1994/20
702 00 Moravská Ostrava

Abstract

The document is focused on the sphere of the complex security policy importance for optimisation and efficiency of security in its widest interpretation. A significant part of the essay is applied to a substantiation of the necessity to have a security policy. The most significant reasons why it is essential to process it are a provision of synergies of individual security subsystems and taking the responsibility for increase of the security level by the department management as well as by all its employees. At the same time it is necessary to realize that a complex security policy is one of the foundations for processing of information-communication technology security policy and implementation of information security management system. Main attention is paid to specific aspects of security policy creation in state administration departments, central administrative bodies and regional authorities. The accent is put on reasoning of the necessity and presentation of a possible attitude to a security policy creation in the sphere of the Ministry of Defence of the Czech Republic. Attention is paid to the definition of the meaning of the security policy term itself and to the analysis of its functions and principles.

The process of creation as well as implementation of the security policy of central administrative bodies and regional authorities is treated as a system, as an open modular process, the success of which is conditioned with application of project methods of its creation process (specification of its main phases; setting its objectives and contents; optimisation of operating methods). Possibilities of outsourcing for security policy creation (design and consultancy services) as well as for its implementation (outsourcing of certain functions of security management) are also taken into account. Security policy has a similar importance for private entities, mainly for those ones that belong to a part of the critical infrastructure of the Czech Republic. For those entities the document has mainly a methodological meaning and it should be applied on specific conditions and branches of business.

Keywords: Security; Security system of the Czech Republic; Critical situations; Preparation for management in critical situations; Crisis management; Security policy; Security policy functions; Security policy principles; Security management; Security policy process creation; Security policy implementation process; Outsourcing of certain functions of security management

1 Historical Context of the Czech Security System Creation with Regard to the Given Topic

This essay´s aim is to draw up the experience from design and consultancy activities focused on security policy creation with an emphasis put on security policies of central administrative bodies and regional authorities.

It is obvious that creation of long-term valid security policies at the levels of central administrative bodies and regional authorities is an important condition for the Czech security system development. It is becoming apparent that drawing up security policies is a step which (with a different level of emergency, though) all central administrative bodies and regional authorities, including the Ministry of Defence of the Czech Republic, shall face.

There it is necessary to introduce briefly the process of legislation creation related to the security system of the Czech Republic. It is useful, since it makes the positive changes that have been done since 1989 on one hand, and the problems that have not been fully solved yet on the other hand more visible.

The Act No. 2/1069 of the Code on Establishment of Ministries and Other Central State Administration Bodies of the ČSR as amended (further referred to as the "Competency Act") provide the widest context for this. The Ministry of Defence of the Czech Republic makes an unsubstituable element of the Czech security system.

The security system is formed by certain elements of legislative, executive and judicial power, municipal authorities as well as legal and physical entities that are responsible for provision of security of the Czech Republic.

The following milestones can be set in the process of the security system creation in the Czech Republic after 1989:

Year/Period	Event
Amended legal rules valid before 1989	Constitution of the Czech Republic; Act No. 2/1969 of the Code on Establishment of Ministries and Other Central State Administration Bodies of the ČSR as amended [1]
Time period 1991-2000	Acceptance of elementary laws setting legislative foundations of the security system of the Czech Republic [2]
2003	Acceptance of the Security Strategy of the Czech Republic [3]
2004	Acceptance of the Czech Army Doctrine [4]

That development brought new views of the following questions:

- elementary specification of the contents of the term "security";
- basic values, interests, attitudes and ambitions of the Czech Republic for provision of security;
- security system of the Czech Republic (definition of the elements of the Czech security system; their structures; specification of security roles and duties, competencies and responsibility for synergy within the system);
- involvement of the Czech Republic into international security structures, undertaking a part in provision of security within them and creation of conditions for efficient cooperation at that level;
- security within individual elements of the Czech security system as one of the basic preconditions for keeping the continuance of the ability of the element to function during critical (crisis) situations.

During those periods the view of security as a process of preparation for critical situations (emergency situations – as a legislative tool responding to them) of military and non-military character, system of

emergency planning and two elementary approaches to it in general have been established. Security itself is understood in the following two ways as:

1. security related to military threats and risks (military policy of the Czech Republic; military preparation of defence, The Army of the Czech Republic, The Ministry of Defence of the Czech Republic as the central body of state administration);
2. security related to non-military threats and risks:
    - preparation for solving critical situations (threats creating crises and risks potentially related to the interests of the Czech Republic, integrated emergency system; central bodies of state administration; regional authorities);
    - preparation for solving critical situations at municipal levels;
    - preparation for solving critical and emergency situations at the level of a company, organization and institution.

Although a great change related to quality in the above-mentioned areas has been made, certain tasks to be completed still remain, above all the following ones:

- need of system changes in the approach to security face to face to new security threats;
- need of system changes in the approach to security face to face to new economical and organizational conditions in which central administrative bodies, and the Ministry of Defence of the Czech Republic as well, work and meet their social functions.

As far as the Ministry of Defence of the Czech Republic´s point of view is concerned, there is an obvious disproportion related to the level of conceptuality of solution of its own external functions (see the above-mentioned "Competency Act") and attention paid to its own security. In this respect, the Ministry of Defence of the Czech Republic is in comparison with some departments even slightly behind. Such condition appears, for instance, in physical security that largely depends on physical guarding, and extent of safeguard technology application, where the level of their integration does not correspond to contemporary trends any more.

A necessity to change the attitude to security of central administrative bodies themselves, organizational parts of all state administration departments and regional authorities, provision of critical internal mechanisms conditioning the continuity of their work, establishment of internal security systems and security management are some of possible tasks resulting from the above-stated problems.

Such a change of the attitude shall be characterized with the following features:

- emphasis on conceptuality of the creation and development process related to security systems of central administrative bodies (middle and long term process);
- observance of specific aspects of security in state administration;
- emphasis on optimization (security; economic; and organizational).

Experience show that a new analysis of security risks, hand in hand with a complex security policy, are the basic tools how to achieve the above-mentioned. Public resources state that just the following institutions have already processed their security policies:

- The Office of the Government of the Czech Republic;
- The Ministry of Internal Affairs of the Czech Republic;
- The Ministry of Foreign Affairs of the Czech Republic;
- The Ministry of Justice of the Czech Republic.

There are the main reasons for processing a complex security policy:

- complex security policy serves as a foundation for implementation of information security management system;
- provision of synergies of individual security subsystems including disposal of duplicate costs;
- optimization of security costs further to a threat and security risk analysis. Replacement of potential risks with real ones;
- setting the intended security level for a longer time period;
- introduction of a unified security management system and responsibility for security;
- declaration of department management responsibility for security and increasing its level;
- definition of the security management role and its competencies;
- introduction of a safety check system and periodical evaluation of its level;
- harmonization of security with legal and expert standards of the Czech Republic, the European Union and NATO;
- creation of space for outsourcing of security processes and services as well as their supervision and quality monitoring;
- definition of a basic standard of physical security with respect to the absence of legislation in this area.

2 The Essence, Functions and Principles of Security Policy

Security policy of central administrative bodies is understood as a document of a conception character with which the central administrative body management, the state administration management or the regional authority management declare their support for the culture of security and for creation of their internal security systems. It is ranked among long-term-valid conception documents of the top management and in this sense it is fully obligatory for all organizational parts and employees.

In our interpretation, the security policy shall meet the following main functions:

- The safety function that expresses the meaning and contents of creation, functioning and development of the security system of central administrative bodies and organization and security process management itself. To understand this meaning and contents of the following security policy functions it is crucial to: perceive security as an constantly open process; permanent trial to optimize the rate between the threats and measures taken; permanent attention paid to all elements of the security system (people; technologies; organization and operating rules) and optimization of performance synergies resulting from their interconnection.
- The program function, the contents of which is mostly focused on: long-term orientation towards security as one of the key items of the creation, functioning and development program; defining the intended security level in context with threats, risks and their tendencies of development; setting the key areas of security; setting measurable objectives.
- The organization function comprising especially: understanding security as an integral part of all managing processes (to include the security aspect into all strategic conceptual decisions; inclusion of security aspects into all levels of process standards); incorporation of organization and security process management into the organization structure; acceptance of a schedule of measures to be taken to improve security; definition of monitoring of their taking; allocation of adequate resources and defending those resources against consequences of later non-conceptual operative changes; acceptance of metrics for the results reached; systematic monitoring and adequate response to findings; acceptance and observance of transparent rules for selection of suppliers.

- The cultural function (to be understood as "company/institution" culture) that means mainly: attention paid to systematic change of the attitude of its employees and hence of the entire institution to security; development of the ability not to be governed by extreme moods, overcoming the feeling "do not panic, everything is all right" on one hand and overcoming feelings of hysteria on the other hand; giving adequate level of importance to all aspects of security and appraisal of work of people providing security; development of willingness to respect certain degree of limitations and discomfort in the interest of safety.
- The political function that expresses an objective power of security as a topic with a strong political potential.

2.1 Elementary Principles of Security Policy:

The Principle of Liabilities. This principle means that each employee of central administrative bodies is obliged to participate in safety (i.e. protection of life and health of persons; property and information; environment; good reputation and other rightful interests). No one is relieved from general liability in principle. The way that the employee shall contribute to protection of rightful interests of the central administrative body is defined in its organization regulations, status of the departments and work statement for individual positions.

The Principle of System Approach. This principle means to require the understanding as well as practical performance of all safety measures not as a series of separate and isolated tasks but as a mutually complementing and supporting system of unified effort. It demands functional cooperation of persons and departments, setting the hierarchy and respect of individual measure importance as well as the hierarchy of competencies to decide, related to activities with various security meanings. Only a strictly given limited number of persons can decide about activities with a special security importance.

The Principle of Factual Liability. This principle means to appoint a certain person to be responsible for security processes. Each person has his/her particular place in the security system of central administrative bodies within which he/she is given particular duties and is personally responsible for satisfying them.

The Principle of Monitoring. Meeting this condition is the elementary precondition for functioning and development of the security system. This principle means that organization and management of security processes includes a system of permanent monitoring and checking the entire system as well as individuals and their activities. A complex security audit is one of efficient forms of monitoring.

The Principle of Evaluation. Periodical evaluation of current level of security is a precondition for its improvement. The outputs are then used for conceptual and personal work and are one of the tools serving for consolidation of security.

The Principle of Flexibility. The central administrative body security system shall be able to react to a change of a security situation, either a general one or in individual departments (workplaces), in a flexible way.

The Principle of Law means that the central administrative body security is based on such standards and procedures that respect and use the legislative framework of the Czech Republic. Mainly in cases when the rights of entities (physical; legal) are restricted in the interest of security, such restrictions shall correspond with legal standards.

3 The Process of Security Policy Creation

An introduction of the central administrative body security policy in not an easy and quick process. The experience has proved that the successfulness of the process depends on a reasonable extent of the three following stages [5]:

3.1 1st Stage: The Stage of Concept Resolution.

Within this stage, mainly those key steps are specified, the negligence of which would cause numerous internal conflicts in the process of security policy creation, would make the process slow and would influence the results of the entire process (usually so that a great deal of security areas logically related would be excluded from the document):

- acceptance of the security policy necessity;
- consideration of the security policy creation method;
- resolution to create a security policy.

3.2 2nd Stage: The Stage of Security Policy Creation comprises especially the following steps:

- definition of crucial security objectives;
- definition of protected assets areas;
- security threats and risks;
- adoption of the security policy conception (structure; structuring);
- organization of an internal discussion (opponencies);
- completion of the final form of the security policy;
- acceptance of the security policy by the department management.

There is a possible example of the security policy structure contents for the central administrative body (department) or regional authority:

- General starting points of the security policy for central administrative bodies (departments) or regional authorities (characteristics of external and internal security environment; general principles of the department security policy; security objectives of the department and their hierarchy; elementary – general security objectives of the department; terminology; abbreviations).
- Security policy of central administrative bodies (departments) or regional authorities (structure and definition of the security policy areas: rules for structuring the areas; structure of the security policy areas; protection of lives and health of persons and property; protection of classified information; security of information and communication systems).
- Starting points of the security policy for central administrative bodies (departments) or regional authorities (legal environment, assets; security management; current situation of security).
- Definition of objectives and desired benefits (elementary objectives; objectives in individual areas of security policy; desired benefits; expenses).
- Areas of security policy: (a) protection of persons and property; b) crisis management; c) safety and protection of health at work and fire protection; d) protection of restricted facts; e) protection of special facts; f) protection of personal data; g) security of information and communication technologies; e) security management – in all the above-mentioned areas: current condition; required final condition; measures to achieve the required condition).

3.3 3rd Stage: The Stage of Practical Implementation of the Security Policy that comprises mainly the following steps:

- processing a schedule of the security policy implementation;
- security policy implementation management.

There is no space for a detailed analysis of the contents and connections now, therefore I am going to add only several notes to the contents of the above-mentioned stages and steps.

The stage of the concept resolution may seem to be rather simple and as far as its contents is concerned even trite (the contents can be specified as "Yes-No-Why"). Nevertheless, this phase is the most important one as well as often the most difficult to implement, which is largely for the following reasons:

- security policy is not a standard yet, and central administrative bodies are not obliged to implement it by any regulations. Justness to undertake this direction is grounded only on general rules of complicated multi-factor process management and standards in the area of information safety;
- the Ministry of Defence under the influence of numerous occupational stereotypes of thinking does not have to perceive its own safety (as one of the central administrative bodies) as a complicated process;
- the Ministry of Defence, although its staff does not comprise professional soldiers only any more (as it used to be in the past) does not have to feel the necessity to accept the security policy also since it has a rather good military regulations, with regard to contents and internal directive acts at their disposal.

These reasons seem to be highly logic at first sight. They appear to be based on the exceptionality of the department of defence within the security system of the Czech Republic. Considering that it is necessary to rely on the sense of conceptual management and reasoning founded on the following indisputable facts:

- Horizontal cooperation of central administrative bodies with one another followed by vertical cooperation with regional authorities and other entities (especially with certain legal entities) is the elementary principle of functioning of the security system of the Czech Republic. Security policy has its specific place in the organization of such cooperation.
- Security is a political affair, political charge of central administrative bodies and the Ministry of Defence in particular is even doubly one, which has its impartial side of the matter. Each underestimation of security at the Ministry of Defence might have a far more larger impact on security of the Czech Republic than at other central administrative bodies or at regional or legal entity level. The subjective side of that results from e.g. considerable attractiveness for media (not limited to the press, TV etc.).
- Central administrative body security level is influenced in many respects by security technologies and therefore it is expensive. Creation of a central administrative body security system and not having a long-term conception is even more expensive (failures of technological continuity; generation change planning, etc.).
- The area of each central administrative body, with no exception for the Ministry of Defence, comprises a great many organization elements. Absence of security policy as well as in certain cases of legislation in force (e.g. in the sphere of physical security) increases the difficulty of their security standardization (and in this respect the security policy is really irreplaceable – see Figure No. 2; in detail).

There is another question of the first stage that seems to be simple at first sight and this is **the question of selection of the security policy creation method**. To solve this task, the central administrative body management considers the following:

- to ensure the security policy creation using its own means or using a supplier (logically it also might be a combination of the above, however, this is the least suitable way that cannot be recommended);

- supplier solution gives numerous advantages, especially the advantage of a qualified view from "outside" ensuring considerably higher objectivity level;
- making good use of potential advantages of a supplier solution is, however, conditioned with the choice of a suitable supplier which is based on a quality definition of requirements on professional, technical, economical, financial and qualification qualities of the applicant.

A possible procedure for processing and implementation of a complex security policy is demonstrated on the example of the diagram on figure 1.

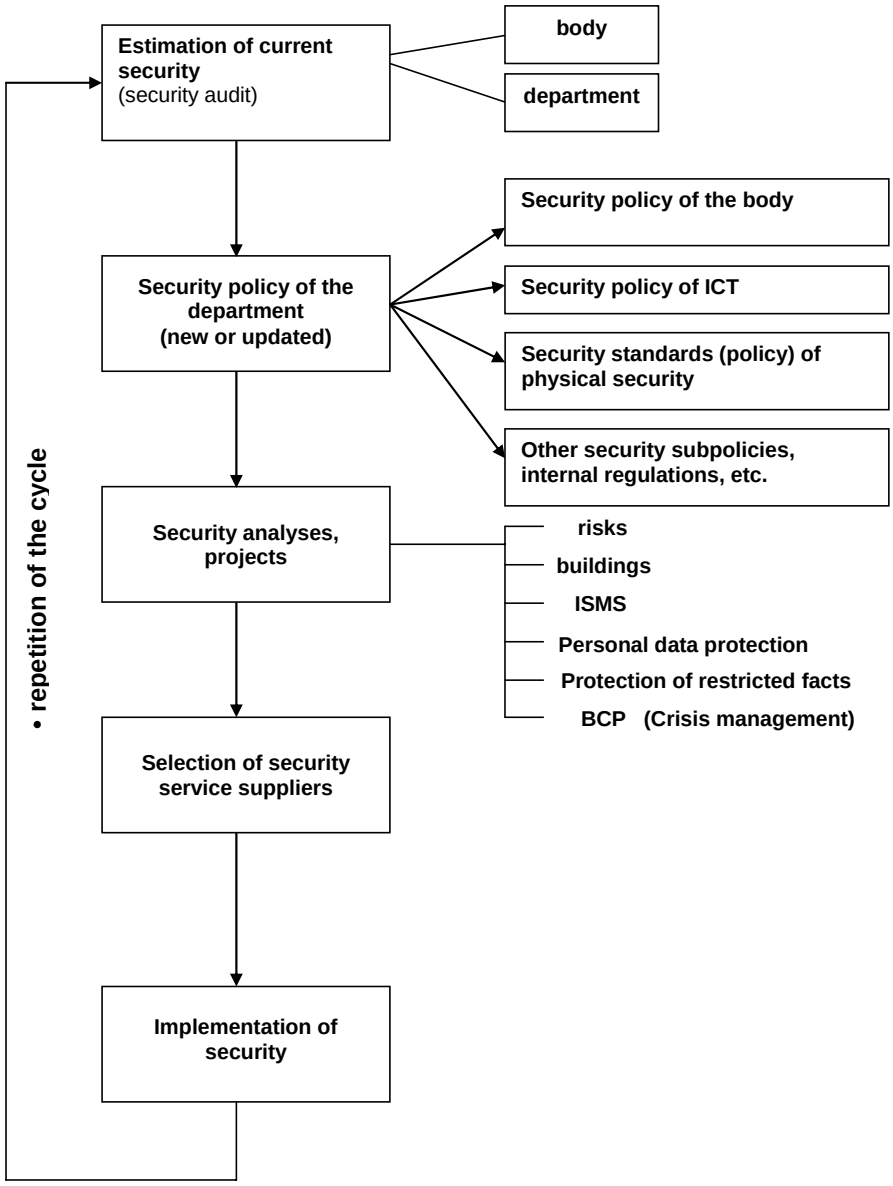

Figure 1: Procedure for processing and implementation of a complex security policy diagram.

4 Security Policy as a Way of Efficient Change of the Attitude to Security Management

Security policy within central administrative bodies (see Figure 2) may, among others, mean a step forward a positive direction in the question of reconsideration of the attitude to security management. In this connection, security management can be understood both its possible ways. In the personnel-organization meaning it can be understood as a group of people responsible for organization and management of security processes and in the meaning of a theory of a control cycle the rationally just view of a controlled process behaviour (in our case security).

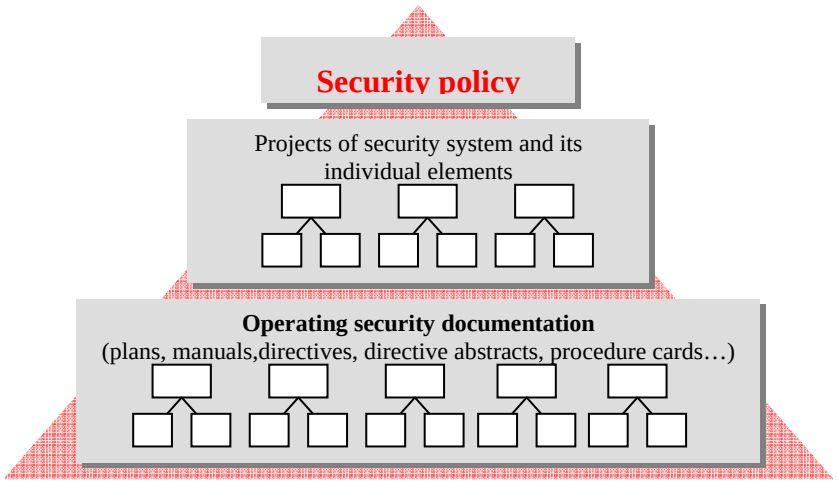

Figure 2: Structure of central administrative body security standards.

Positive potential of the security policy impact on security management in the personnel-organization meaning can be seen in the fact that it provides a long-term perspective (structure; special training; organization incorporation; synergy relations).

In the meaning of the rationally just view of a controlled process behaviour it especially:

- provides a support for decision making processes in the sphere of safety (security policy is a strategic document of management and in this sense it has the authority enabling simplification when surmounting immediate adverse conditions);
- security policy makes the allocation of budget resources with a better perspective easier;
- it facilitates adequacy of the expectations (with respect to the stage of the implementation; with respect to a substantiality of the managing interference; with respect to a step by step specified level of required security in individual stages of implementation; makes rational prediction of acceptable deviation of the system behaviour after a management interference etc. easier – for details – see Figure 3).

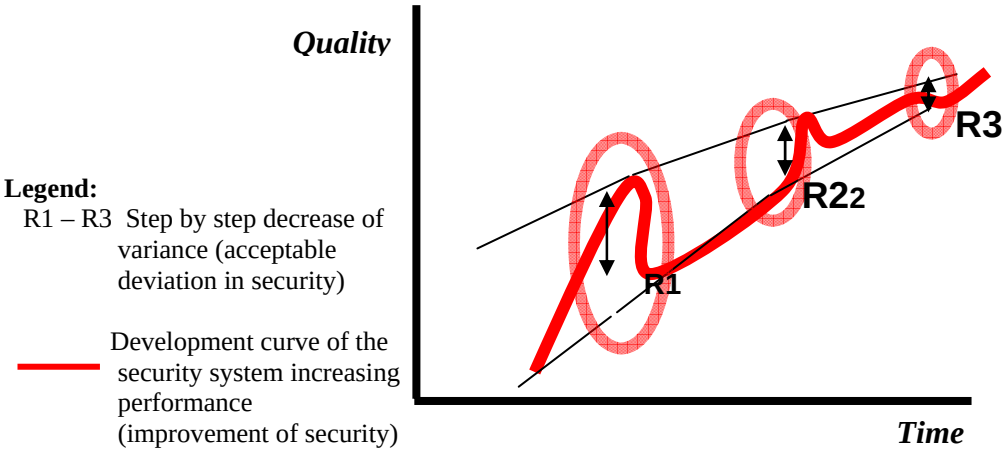

Figure 3: Behaviour of the controlled security system after a management interference.

5 Possibilities of Security Management Outsourcing

There is the space now for detailed attention paid to one of the key questions of security management – the question of possibilities to outsource its selected functions.

Generally speaking, the experience prove that this is one of the possibilities how to increase the professional quality of the security management and at the same time to optimize its organization and cost aspects. However, respect to certain conditions is a must. The most important ones comprise the following:

- consistent monitoring executed by the customer that ordered the outsourced services (central administrative bodies; regional authorities);
- use of applied procedures of facility management when setting the organization structure of outsourcing;
- right setting of the evaluation criteria for the offers in tenders.

Preconditions of continual supervision executed by the customer that ordered the outsourced services mean to ensure the position of the outsourced service coordinator that is skilled and informed about the condition of the outsourced functions (a possible variant of organization structure can be seen below – see Figure 4)

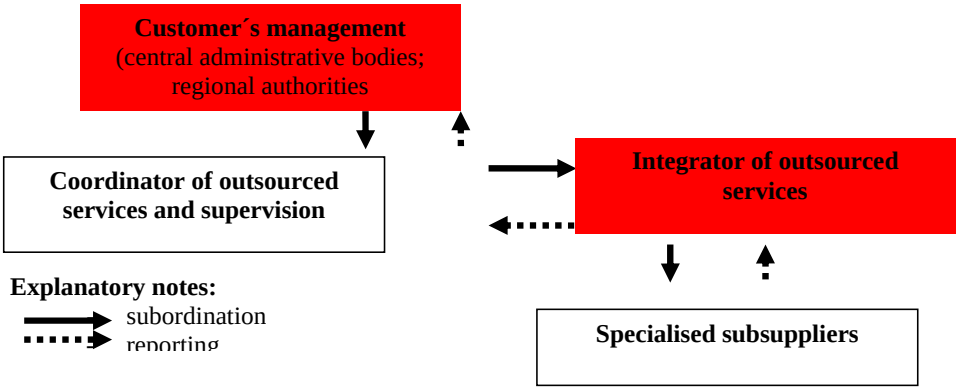

Figure 4: Optimum diagram of the organization of the relation between the customer – supplier from the point of view of monitoring continuance and the customer´s readiness to act.

Readiness and awareness of the coordinator of the security management outsourced functions comprises especially the following items:

- availability of complete and updated security documentation;
- understanding of security system functioning;
- professional competence to temporarily ensure the continuance of the security system functioning in case that the integrator of the outsourced services looses the ability to work.

Use of the applied procedures of facility management when **setting the optimum organization structure of outsourcing of certain functions of security management** comprises especially the following items:

- keeping a strict hierarchy of relations in accordance with Figure 4;
- treaty reinsurance of the relation customer-supplier (integrator) and supplier (integrator) – specialized subsupplier including conclusion of a treaty on quality of the services provided (Service Level Agreement);
- when selecting specialized subsuppliers, the supplier (integrator) shall be given a free hand to select (limited only by basic conditions stipulated in the contract with the customer, including obligatory documenting of the selection);
- to use mainly economical tools (yearly budget; quarterly balancing cycle of its drawing) and quality tools (contractual definition of required security level and its reflection in the Service Level Agreement metrics) for management of the extent and functioning of the outsourced services on the part of the customer.

The conception of the Service Level Agreement is vital for permanent monitoring of the quality of certain outsourced functions of security management, above all the following items:

- periods of evaluation;
- definition of quality indicators (metrics) and definition of an acceptable deviation;
- setting of the penalty mechanism.

Right setting of the evaluation criteria for offers in tenders for the integrator of outsourcing of certain functions of the security management consist of especially the following items:

- optimization of the relation among individual selection criteria, mainly between the price and other criteria;
- adequate emphasis on security criteria.

At the same time it is necessary to realize that an overall security outsourcing or security management outsourcing is not possible within specific conditions of the Ministry of Defence and other central administrative bodies handling with restricted information. Moreover, close attention shall be paid to supervision and to quality monitoring of the outsourced services.

One integrator´s of all outsourced activities vision does not have to be accepted for number of reasons. Integration of individual security subsystems, e.g. technical safeguards, guarding, fire protection and security and health protection at work is a more acceptable form.

Possible space for consultancy companies in the sphere of security management outsourcing present not only one-shot activities related to processing of analyses, studies and security documentations, but also the following ones:

- administration of technical safeguard systems (position of a responsible person according to the ČSN EN standard, series 5013);
- quality monitoring of the following outsourced services: physical guarding and technical safeguard, (professional takeovers, audits and performance checks);

- outsourcing of project manager positions in the stage of implementation of safety measures;
- outsourcing of regional positions of security management.

Provision of the suppliers´ security competencies for such outsourcing and a demand on processing of their plans for business continuity act an important role.

We are convinced that acceptation of a long-term valid security policy together with modern forms of outsourcing are the key methods how to increase security of all central administrative bodies and regional authorities leading to intensification of their ability to fulfill their roles in the security system of the Czech Republic.

Requirements to introduce the security policy implementation process in the sphere of the Ministry of Defence as well as in other central administrative bodies have been becoming more and more topical with respect to increasing costs and demands of cost reduction. Now the time, when a purposeful management of security risks is not possible without implementation of a complex security policy, has come.

References:

[1] Act No. 1/1993 of the Code, the Constitution of the Czech Republic.

[2] Act No. 240/2000 of the Code on Crisis Management as amended (crisis act); Act No. 241/2000 of the Code on Economic Measures for Critical Conditions as amended; Act No. 239/2000 of the Code on Integrated Emergency System as amended; Act No. 238/ 2000 of the Code on Fire-brigade of the Czech Republic as amended; Act No. 222/1999 of the Code on Provision of Defence of the Czech Republic; Act No. 283/1991 of the Code, on the Police Forces of the Czech Republic; Act No. 219/1999 of the Code on the Armed Forces of the Czech Republic; Act No. 129/2000 of the Code on Regions (establishment of regions).

[3] Bezpečnostní strategie ČR (Security Strategies of the Czech Republic), Praha 2003.

[4] Doktrína Armády České republiky (Doctrine of the Army of the Czech Republic), Ministerstvo obrany České republiky (the Ministry of Defence of the Czech Republic), Praha 2004.

[5] Fryšar, M. a kol. (at al.): Bezpečnost pro manažery, podnikatele a politiky (Security for Managers, Businessmen and Politicians), Public History Praha 2006, ISBN 80-86445-22-4, s.13;35; 51-69.