EXAMPLE OF SECURITY MANAGEMENT SYSTEM OF THE ORGANIZATION – COMPONENTS AND CONCEPTS

ПРИМЕР НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ОРГАНИЗАЦИЯТА – КОМПОНЕНТИ И КОНЦЕПИИ

Dr. Eng. Dimitrov D.L., Dr. Eng. Panevski V.S., Nikolov G.M.
Institute of Metal Science Equipment and Technologies "Acad. A Balevski" with Hydroaerodynamics Centre - Bulgarian Academy of Sciences, Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg; panevski@ims.bas.bg; g.nikolov@ims.bas.bg

Abstract: Issues related to security are intertwined in all areas of the life of an organization. Many of them are considered and documented organizational and provided within the respective area/subsystem of the management system of the organization. For example, information security management is detailed and reliably described in the international standards. And this is natural, considering the importance of this type of security and the fact that information technology lie at the core of almost all organizations. In the meantime however, it is necessary to go a long way to reach the ultimate goal of improving security of the organizations by developing integrated management systems for business security. A Security Management System may be considered as that part of the overall management system, based manly of the quality management system, that provides the structure to enable identification of potential threats to an organization and which establishes, implements, operates, monitors, reviews and maintains all appropriate measures to provide assurance of the effective management of the associated security risks.

KEYWORDS: QUALITY; QUALITY MANAGEMENT SYSTEM (QMS); SECURITY; SECURITY MANAGEMENT SYSTEM (SMS); INTEGRATED MANAGEMENT SYSTEMS FOR BUSINESS SECURITY; SECURITY RISKS.

1. Introduction

Successful companies have found a way to offer something that people want, at a price they are willing pay, in a way that will make money in the transactions. Highly successful companies offer quality products and services in this exchange, and keep quality high; so that the customer will return the next time he/she wants to purchase **[1].**

Quality has been defined as "The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs. Not to be mistaken for "degree of excellence" or "fitness for use" which meet only part of the definition". By this definition, security is a component of quality.

Security is defined by the American Heritage Dictionary in their on-line database as:

a) Freedom from risk or danger, safety;

b) Freedom from doubt, anxiety or fear; confidence;

c) Something that gives or assures safety as:

- a group or department of private guards;
- measures adopted by a government to prevent espionage, sabotage or attack;
- measures adopted, as by a business or homeowner, to prevent a crime such as burglar or assault.

These definitions, taken together, can demonstrate that quality is the responsibility of the whole organization and security is a part of the totality of quality of a system, implicit in customers` expectations. Security, as a component of quality, must be addressed throughout an organization, in the definition of strategy, the development of policy and the implementation and monitoring of both **[2].**

2. Components of security management system - discussion

Component 1 – Credibility and Integration of the Personnel

A prerequisite that corporate security personnel come, for example, from military, intelligence or law enforcement background, it is essential that those with responsibility for security are able to demonstrate competence not only in all aspects of the security discipline, but also have an awareness of the contribution security can make to other aspects of the business, such as Governance, Strategy, Compliance, Assurance, New Ventures, and other essential business-related issues. It is the responsibility of the person with overall responsibility for Security to ensure that training and development needs arc recognized, addressed and records maintained. In this way, security may become an integrated and respected part of the organization; used in business planning, execution, and decision making. Expectations of security personnel are:

- Professionalism - living the corporate values;
- Expertise - demonstrating a thorough knowledge of the subject;
- Vision - demonstrating an understanding of the wider business objectives;
- Teamwork - working closely with other disciplines to understand their contributions and aspirations;
- Collaboration - conducting security risk assessments in support of specific operations, not in isolation;
- Communication - security considerations to top management in a clear, concise manner, demonstrating due consideration to all factors.

Component 2 - Policies, Objectives and Tasks

There should exist a single security policy which outlines the security architecture, strategy and protocols.

The following sections are addressed:

- Security management objectives;
- Statement of the attitude of the organization to security;
- Description of the security environment;
- Statement of the security risk appetite;
- Security organization, roles and responsibilities;
- Procedures for security risk assessment;
- List of security Standing Operating Procedures (SOPs);

- Security priorities and calendar for coming year.

Component 3 - Threat, Vulnerability and Security Risk Assessment

Security risk assessments should take into consideration a wide range of elements beyond physical security threats. Such elements should include:

- The operating environment and groups/events by which it is characterized;
- The profile of the organization, the footprint and the social impact;
- The strategic, long term objectives of the organization;
- Voluntary Principles of Security and Human Rights;
- Legislation and local expectations;
- Capability and intent of local criminal/terrorist elements;
- Vulnerability and attractiveness of assets to criminal/terrorist elements;
- Availability of resources.

Component 4 – Controls

Examples of security controls may include:

- Physical protection measures (lights, fences, CCTV, barriers, etc.);
- Introduction of security procedures (ID checking, access control, mail screening, etc.);
- Intelligence networking (local social/political leaders/intelligence providers, etc.);
- Electronic security (encryption, password protection, etc.);
- Resourcing (security personnel, equipment, etc.);
- Local integration (CSR programme, local content, etc.;)

Component 5 - Security Risk Register

A security risk register should:

- Facilitate ownership and management of security risks;
- Provide an overview of the significant security risks that arc faced by an organization;
- Record the results of threat/vulnerability security risk assessment;
- Form an agreed record of those security risks that have been identified;
- Record additional proposed actions to improve the security profile;
- Facilitate the prioritization of security risks.

Component 6 - Planning and Resourcing

Effective planning will answer:

- What are we going to do?
- How are we going to do it?
- When are we going to do it?
- How long do we need to do it for?
- How are we going to coordinate and communicate?
- What do we do if something goes wrong?

Effective resourcing will answer:

- What do we need to do it?
- How do we get it?
- How much does it cost?
- What is our back up if something doesn't work or isn't available?

Component 7 - Execution and Control Activities

The execution of a plan is predicated on all of the previous components in the management system:

- The plan has identified all the security risks to the operation;
- All control mechanisms are established;
- The plan has been accordingly and appropriately resourced;
- Any bespoke procedures are documented, approved and validated;
- The plan has been effectively communicated to those with responsibility for its execution;
- Assurance that those with responsibility for carrying out the plan have the correct competencies;
- All correct back up and reinforcement strategies are established and tested.

Component 8 - Monitor and Security Reporting

Monitoring is based, upon effective two-way communication. Where appropriate, traditional methods are often effective and should be considered:

- Inspections;
- Review meetings;
- Auditing;
- Interviews;
- Workshops.

Component 9 – Review

The purpose of the review may be any combination of the following:

- To critically debrief the plan in order to determine strengths weaknesses and areas that could be improved;
- To obtain feedback from those involved in the execution of the plan/ project regarding the manageability of the plan;
- To highlight any competency issues arising from exposure to new challenges;
- To examine how much contribution the operation/task/project brings to the achievement of the organization's objectives;
- Assurance to top management that security is being managed effectively;
- Enables security management to assess whether established protocols are being effective, and to take action accordingly;
- Highlight examples of good practice.

Component 10 – Learning

Effective processes for learning lessons will enable an organization to:

- Introduce improvements to procedures;
- Introduce improvements in organizational structure;
- Update documentation;
- Implement of new training courses;
- Increase awareness of new threats/update on existing threats;
- Introduce new equipment/technology;

- Better integrate to the wider organization;
- Better understand the organization's objectives;
- Heightened awareness of the contribution of security;
- Improved relationship with/understanding of other business functions;
- Improvements to the management system;

Component 11 - Reporting to Top Management

Providing such feedback to top management:

- Offers reassurance that security is being effectively managed;
- Offers reassurance that security understands its role in the achievement of the business objectives;
- Gives confidence in decision-making that all security issues have been given appropriate consideration;
- Reinforces the importance of security considerations in making decisions;
- Reinforces the role of security in protecting the organization's people, assets and information;
- Emphasizes that security operates in support of business operations, and not as a barrier to them.

3. Concepts of the security management system – discussions

3.1. Security and Quality Management

A security management system, as with other management systems is based upon the model defined in ISO 9001:2008, Quality Management Systems –Requirements **[3].** In a security risk-based, process-driven approach to security, the achievement of security objectives should start with a threat/security risk assessment. Having identified the security risks and planned mitigation measures, a security risk register may be established. The mitigation measures detailed in the security risk register are realized through resource management and security planning, thus arriving at a security solution (product), whether that is hard security measures, procedural requirements or a higher level security solution that supports strategic objectives, such as a crisis management strategy, or establishment of an intelligence gathering network.

3.2. Documentation and Management Systems

A management system, as defined by ISO 9000:2005 **[4]** is a 'system to establish policy and objectives and to achieve those objectives'. In order to help in the achievement of those objectives, the system needs to be supported; that support comes in the form of approved standards and procedures. An effective management system should be such that it does not necessarily need a discipline expert to implement and manage it.

3.3. Security Management Principles

(a) Customer focus;

(b) Leadership;

(c) Involvement of people;

(d) Process approach;

(e) Systems approach to management;

(f) Continual improvement;

(g) Factual approach to decision making;

(h) Mutually beneficial supplier relationships.

3.4. Security risk Management and Assessment

(a) Definitions

ISO Guide 73:2009 **[5]** provides the following definitions:

Term Definition

○ Risk - effect of uncertainty on objectives;

○ Risk analysis - process to comprehend the nature of risk and to determine the level of risk;

○ Risk appetite - amount and type of risk that an organization is willing to pursue or retain;

○ Risk assessment - overall process of identification, analysis and evaluation;

○ Risk evaluation - process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable;

○ Risk identification - process of finding, recognizing and describing security risks;

○ Risk management - coordinated activities to direct and control an organization with regard to security risk;

○ Risk tolerance - organization's or stakeholder's readiness to bear the risk after security risk treatment in order to achieve its objectives;

○ Risk treatment - process to modify risk.

(b) Security Risk Management Process

The purpose of security risk management may be described as:

"To identify the threats and security risks to an organization and to manage those security risks within the risk appetite of the organization in order to provide reasonable assurance of the achievement of the organizations objectives" **[6].**

(c) Security risk Registers

There is no prescription for the format of a security risk register, which will vary according to the organization's culture, security risk classification systems, the nature of the project, reporting requirements and so on, but the following components are generally considered key:

- Inherent risk: The level of risk before any control activities have been applied;
- Residual risk: The level of risk that currently exists, taking into account controls that have been established;
- Target risk: The ultimate level of risk that is desired by the organization;
- Controls: Measures implemented to modify risk.

(d) Security risk Treatment

A brief mention should be made of Controls. Controls are those measures which effect the security risk treatment. In simple terms, security risk treatment may fall into four categories:

- Treat: apply controls internally;
- Tolerate: accept that risk is already within tolerance levels; no controls required;
- Transfer: pass the risk on to a third party; usually an insurer or a contractor;
- Terminate: decide that even if controls are established, the risk will remain outside the tolerance of the organization, and so a decision to end the course of action that carries the risk would usually be made by top management;

(e) Analysing Likelihood and Impact

There are a variety of formats; some of the more detailed include other categories such as:

• Time before Impact;

• Duration of Impact.

It is for the individual organizations to define their own policies on security risk register format and management.

3.5. Security Excellence

The European Foundation for Quality Management has recently published the latest version of its Excellence Model **[7].** The Excellence Model is a non-prescriptive framework for management systems that has been widely adopted in both the public and private sector. The Concepts of Excellence **[8]** and the criteria may be adapted for security as follows:

3.5.1. Adding Value for the Customer

Security is often perceived as an unnecessary barrier to progress. One way to overcome this and to embed security into daily business is by understanding, anticipating and fulfilling their needs, expectations and opportunities.

3.5.2. Creating a Sustainable Future

In the exploration phase particularly, winning over 'hearts and minds' is often the key to security. An unhappy community in some parts of the world can create significant security risks. Security input to the Corporate Social Responsibility (CSR) programme is therefore invaluable in advancing the social conditions within affected communities.

3.5.3. Developing Organizational Capability

Managing or creating the ability to change the capability of the security organization will enable it to respond/adapt to the different demands made upon it, whether it be deployment of a guard force with limited notice, provision of executive protection, or carrying out security compliance exercises. The security organization must strive to be multi-facetted.

3.5.4. Harnessing Creativity and Innovation

Often, effective security solutions come from creative thinking. There is no textbook solution to security challenges and so security managers must be open to all ideas at all levels, no matter radical they may seem.

3.5.5. Leading with Vision, Inspiration and Integrity

Upholding the organization's values is as relevant to the security function as it is to every other function. Security is not exempt from the need to inspire through upholding moral values. Upholding the Voluntary Principles of Security and Human Rights (VPSHR) is one area where security has the opportunity to show inspired leadership.

3.5.6. Managing with Agility

Being 'agile' in security means having the ability to effectively and efficiently recognize and respond to threats and opportunities. The notion of a Quick Reaction Force, for example follows this concept.

3.5.7. Succeeding through the Talent of People

Teamwork is key in all disciplines, but arguably more so in security; the ability to stand in for each other seamlessly, be it stepping up or stepping down, and achieving coordination in operations through an understanding of each other’s' roles ensures and develops talent and progression.

3.5.8. Sustaining Outstanding Results

In security terms, this translates as providing a 'best in class' support in all areas, and planning now to do the same in the future. Resource and strategy planning for new country entry well in advance is an example where security could sustain an outstanding performance.

Conclusion:

Obviously, the four most important characteristics of any operational management system are:

- Leadership;
- Security risk Management, Implementation;
- Continuous Improvement.

This is consistent with the fundamentals of security management, and so these characteristics also form the hub of the Security Management System (SMS) wheel.

Effective implementation of the SMS will ensure:

- Confidence - that security has the ability to prepare for and react to events that may otherwise present a threat to the organization's people, information and/or assets;
- Optimization - that the most efficient use of resources is made at optimum cost;

In contributing to the organizations overall Confidence levels and Optimization of resources, a SMS will:

- Improve the resilience of the organization;
- Enhance the organization's credibility;
- Introduce a core language and core processes for security risk management;
- Enable an organization to be nimble and flexible in its response to security challenges;
- Continually improve the capacity of an organization to manage security challenges.

Literature:

1. OGP, Operating Management System Framework for controlling risk and delivering high performance in the oil and gas industry;

2. OGP, Processes and concepts in security management;

3. ISO 9001:2008 - Quality Management Systems - Requirements Summary;

4. ISO 9000:2005 - Quality Management Systems - Fundamentals and Vocabulary;

5. ISO Guide 73009 - *Risk management -- Vocabulary*

6. ISO 31000:2009 - Risk Management - Principles and Guidelines;

7. EQFM Excellence Model, EFQM Publications, 2012;

8. Fundamental Concepts of Excellence, EFQM Publications, 2012;