REGIONAL DEPARTMENT
OF DEFENSE RESOURCES MANAGEMENT STUDIES

THE 3rd EXPLORATORY WORKHOP

"INFORMATION RESOURCES MANAGEMENT - ISSUES, CHALLENGES AND FUTURE TRENDS"

ISSN: 2286 - 3060

ISSN-L: 2286 - 3060

COORDINATOR:

Senior Lecturer Ph.D. eng. **CEZAR VASILESCU**

National Defense University "Carol I" Publishing House
Bucharest 2012

THE 3rd EXPLORATORY WORKHOP
"INFORMATION RESOURCES MANAGEMENT - ISSUES, CHALLENGES AND FUTURE TRENDS"

WORKSHOP COMMITTEE

LTC Cezar VASILESCU, Senior Lecturer PhD. Eng.
Maria CONSTANTINESCU, Lecturer PhD.
LTC Daniel SORA, Military Professor PhD.
Aura CODREANU, Junior Lecturer PhD.

SESSION CHAIRMEN

LTC Cezar VASILESCU, Senior Lecturer PhD. Eng.
Maria CONSTANTINESCU, Lecturer PhD.
LTC Daniel SORA, Military Professor PhD.
Aura CODREANU, Junior Lecturer PhD.

THE 3rd EXPLORATORY WORKHOP
"INFORMATION RESOURCES MANAGEMENT - ISSUES, CHALLENGES AND FUTURE TRENDS"

07 November 2012

Proceedings of the workshop unfolded during the

Postgraduate Information Resources Management
Course for Senior Officials

Conducted by the
Regional Department
of Defense Resources Management Studies

01 October - 23 November 2012

Braşov
ROMÂNIA

This page is intentionally left blank

WORKSHOP CONTENTS

This page is intentionally left blank

IMAGE CRISIS MANAGEMENT THROUGH PUBLIC RELATIONS

Cpt. cdor. Lucian MOLDOVAN

CONTENTS

IMAGE CRISIS MANAGEMENT THROUGH PUBLIC RELATIONS

INTRODUCTION

Everybody has a public image. That's a fact, so nobody can choose whether to have this image or not. All that matters is to know how to manage to get the best benefit of that image. As individuals, organizations are judged by the impressions they make on the public. The market position of any organization depends on the image of its brand. Depending on the brand image and according to his tastes, the client goes to an organization or another.

The premise from which we started while writing this paperwork was that "we are not an image, but we have an image" and the full involvement of the organization in creating and maintaining a good public image serves better its interests than assisting passively while the image is getting formed at random.

A good image of the organization has great influence on its success and perception among the general public. On the contrary, a negative image can affect the corporate success. Therefore, improving the quality of public relations in order to manage efficiently the organization's image, contributes decisively to enhance public confidence in it and in its development.

I. SOCIAL IMAGE AND BRAND IMAGE OF AN ORGANIZATION

The human being is able to create and operate consciously with images, symbols or pictures. This is an attribute of the human superiority in the universe and a way to develop the human thinking.

In today's society, the image of an organization is considered as an object of patrimony, no matter if it's inherited, included in the total assets of the organization, or regarded as an immaterial (subjective) dimension. Therefore the leaders care more and more about creating and maintaining a good public image and efforts continuously increase in this respect.

Roger Muchielli defines image as "the representation or the idea made by individuals coming from a certain environment or from a segment of the public"

further to the perception of certain information on a social object. "The picture does not designate a fixed item, but a direction, a way to organize information."[1].

In my opinion, the image of an organization is the sum of beliefs, ideas and impressions that people have about that organization. The images represent a product of our mind and are a simplification of much information about that organization. An image is formed gradually through the information obtained and gets deformed over time.

The image of an organization consists of the following overlay:

- the image of the organization as perceived by itself (subjective elements);
- the image of the organization as transmitted to the world (the transmission of information);
- the image of the organization as perceived from outside (the response to the transmission of information);
- the image of the organization as it would like to be perceived (the ideal image);
- the organization as it actually is (a fact literally impossible to communicate).

Marketing studies have concluded that, in fact, consumers eat, drink and wear images. People choose products that best express the role and status they hold in society. Thus, brands have the quality of symbols of that status.

If someone perceives himself / herself in a positive way, he or she will not buy a product that has a negative image, or a product made by a company with a negative image. Also, an individual's good image of a product is not enough. It is necessary that the product be positively perceived by a group of individuals, because each individual needs appreciation, esteem and the feeling that he belongs to the group.

It is important to make a distinction between identity and image. "The identity refers to the way an organization seeks to identify itself while the image is the way the public perceives the organization."[2].

Everyone has a shadow, as well as a sparkle in the eye, which are only his. Every woman has something different, some unmistakable features. Each person has a brand, often worn unconsciously. The same goes for the organizations.

The brand is defined by the American Marketing Association as "a name, a term, a symbol or a design, a combination of these elements intended to help identify

---

[1] Bogdan Teodorescu - *Marketing politic şi electoral*, Editura SNSPA-Facultatea de Comunicare şi Relaţii Publice, Bucureşti, 2001, pag.170

[2] Philip Kotler - *Managementul marketingului*, Editura Teora, Bucureşti, 1997, pag. 389

the goods or services of a seller or group of sellers and to differentiate them from their competitors'. The brand is the hallmark, the summary representation, the identity, style and reputation of the organization. The attraction, trust and rank given by the society depend all on the brand.

"In essence, a brand is a seller's promise to always provide certain products, benefits and services to the customers. The best brands guarantee the quality of goods and services"[3].

The brand manages to individualize a company, a product or a service, enabling the buyer to distinguish them from other similar items. People will memorize a product according to its specific characteristics; they will give them a psychological meaning and will establish affective relationships in their own horizons of expectation. The brand of an organization helps customers to not only locate it, but also to attract them, offering distinct features to a company compared to another.

In this way, branding has replaced, gradually, the reputation of an organization and therefore we can speak of "brand image power" and that's because lately, brands are in fact what people know and buy, as consumers.

II. SOCIAL AND BRAND IMAGE MANAGEMENT

II.1. SOCIAL IMAGE MANAGEMENT

As a result of the communication process, the image helps the crystallization of opinions, beliefs, attitudes and convictions. True or false, positive or negative, the items of information help support modify or reject an idea and have strong influence on human behavior. Messages play a fundamental role in the management of an organization's image. These messages can be:

- Functional ones - results of the organization's activity, characterized by reliability, consistency, stability; can be easily checked, observed.
- Deliberate ones - promoting the image and carrying out the functions of informing, explaining, keeping visible; they are addressing the entire community.

Good image of an organization can be built by first making organization and then what communicates itself. Image of the organization can be managed at least three ways[4]:

[3] *Ibidem*, pag. 558

- Doing good things for the purpose of practicing a highly efficient management;
- Carrying out a professional communication activity and public relations through which to gain confidence, sympathy, understanding and public support;
- Carrying out an aggressive advertising campaign.

The management of the organization's image can be achieved by applying an effective communication policy. The communication policy includes all internal and external measures acting on knowledge, perceptions and public attitudes towards the organization's performance.

The image-building strategies of an organization should aim at creating a positive image by projecting its personality, character and identity within the individual and collective mind. In order to build the image that will be sent to targets, NJ Dougherty and D. Bonanno suggest the following steps:

- Deciding on the parameters of the image about to be projected on short, medium and long term;
- Building a "Statement of image";
- Determining the organization's image in the public's perspective, step involving continuous and systematic efforts to investigate what people think about the organization[5].

Aiming to transmit information about the organization, the promotional activity is a separate component of the communication process. The communication objectives are set according to the organization's marketing objectives and the pursued target groups.

The promotion of the organization's image is meant to submit the following information to the audience:

- The role of the organization;
- The activities of the organization
- The member's role;
- Important events the members attend or events taking place within the organization.

---

[4] Valentin Stancu, *Relaţii publice – curs univ*., Editura SNSPA - Facultatea de Comunicare şi Relaţii Publice, Bucureşti, 2001, pag.4

[5] Virginia Oprişan - *Marketing şi comunicare în sport*, Ed. Uranus, Bucureşti, 2002, pag. 167

So that messages transmit the same meaning and resulted images from different actions be consistent, the organization's image becomes visible by using publicity, advertising, opinion leaders and public relations techniques.

The publicity is an action that aims to enhance the reputation of the organization and is providing information items to the media hoping that they will be judged newsworthy and therefore published for free.

The advertising is the technique used to bring products, services, opinions or causes to public attention in order to convince people to react in a decisive way, as advised by the transmitter. The advertising can be defined as any form of impersonal promotion and presentation of ideas, goods, services or organizations, through words, pictures or sounds. It is paid by a sponsor specifically identified. The sponsor can control the message content and the location of the transmission.

Opinion leaders are part of the opinion maker's category, along with the decision makers and play an important role in the information filtering, perception orientation and attitude formation.

Public relations as a promotional activity preserve a positive image of the product, service or organization.

The evaluation will take into account all relevant images for the organization. There are always more pictures on this, and the images crystallized in information social interpreters can not be summarized nor discriminated by investigating some and ignoring others.

II.2. BRAND IMAGE MANAGEMENT

The market position of any organization depends on the image of its brand. Depending on the brand image and according to his tastes, the client goes to an organization or another. These inevitably imply the settling of that organization's brand image and its efficient management.

The full involvement of the organization in creating and maintaining a good public image serves better its interests than assisting passively while the image is getting formed at random.

An experienced trader said: "*Nowadays, people no longer buy shoes to keep their feet warm and dry. They buy them for the image those shoes creates about themselves - of manliness, firmness, vigor, originality, sophistication, power of seduction, authority. Buying a pair of shoes has become an emotional experience. At*

present, our company sells emotions, not shoes". Therefore, the "brand image power" is what makes the product be purchased.

The personality of a successful brand is object of creation. It is the result of an entire program of creating identities. The identity refers to the way the company makes itself recognizable to customers and the image is the way the public perceives that company. The company creates its own identity in order to mould the consumers` image about itself.

To create a good image for an organization, the brand name is extremely important. It must fulfill the following conditions:

- To suggest something about the benefits offered by the product;
- To suggest product features such as instructions or color;
- To be easily pronounced, recognized and remembered (short names are preferable);
- To be characteristic of the product;
- To avoid misinterpretations in other languages.

"Everyone is looking for particular features in a brand. Therefore the brand image should bear a unique message, suggesting main product quality and market position; the message must be sent separately, to avoid confusion with similar posts from competitors and must have sufficient emotional strength, as to draw buyers` attention and curiosity"[6]*.*

Making a strong brand image requires creativity and hard work. It can't be introduced into people's mind either overnight or using a single mass media item. The image must be transmitted continuously through all available means: using symbols, print and audio-visual media and events.

A powerful image is based on one or more symbols that are meant to help consumers recognize the company or brand. Logos should bring to instant recognition of the company or brand. Advertisements must submit a plot, a mood, a performance, something special.

If the image (mark) of an organization needs to be changed, this should be done with caution and at the right time. Otherwise, quick identification symbols will be lost and, consequently, the ability to attract customers will decrease.

III. ORGANIZATION'S IMAGE MANAGEMENT THROUGH PR

III.1. ORGANIZATION'S IMAGE MANAGEMENT IN DIFFERENT ARES

The organization manages its image through a solid public relations work, involving communication techniques in the following areas: internal information (personnel information), external information (information and connection with audiences outside the organization), relations with the public and relations with the society.

A fundamental principle of public relations says that "public relations begin at home". The meaning of this statement is that if internal information is not carried out properly, the organization can not conduct fair and consistent relationship programs with the company. An undeclared goal is that, when talking about the organization, members should represent "one voice, telling the same consistent message."

The external information comprises the connection with the community, with the mass media and the informing process within an international environment.

In order to ensure a good visibility, the organization normally needs to publish information about itself. The most commonly used methods for transmitting press information are the following: the interview; the press conference and the briefing.

The communication remains the main purpose of the relationship between companies and society[7]. People currently judge the whole considering the details they can see. While talking about relationships between companies and society, the most used methods are the organization of events, the participation in social activities and sponsorships.

III.2. PUBLIC RELATIONS – ROLE, DEFINITION, PRINCIPLES

When an organization or a person will try to establish relations with public, they will practically use public relations. Public relations have been used by necessity. In order to be part of a society, to protect yourself from attacks, to be able to share your points of view, you must know how to speak, you must learn how to listen and be able to communicate. The role of public relations came out from the need to exist, the wish to appear and fear to disappear.

---

[6] *Ibidem*, pag. 389
[7] Valentin Stancu, *op.cit.*, pag.81

Public relations are necessary in order to communicate, to draw attention, to inform, to create a climate of sympathy, to solve problems, to manage challenges, to develop an image, to defend, to influence public opinion, to answer journalists and people, to face social-economic complexity.

In short, according to the UK's Institute of Public Relations, PR activity focuses on:

a. Ensuring a consistent image of the subject;

b. Shaping and maintaining the best possible image;

c. Maintaining good relationship with various organizations or internal/external bodies;

d. Conducting lobby activities in favor of the subject;

e. Ensuring internal and external communication.

In the past, there have been many attempts to define public relations. The most famous ones are: one was given by the British Institute of Public Relations (a), the other one represents the opinion of the International Public Relations Association (IPRA) (b):

a. the Public Relations represent a planned and sustainable effort to establish and keep a state of sympathy and understanding between an organization and its environment.

This definition emphasizes the importance of planning and mutual understanding, a two-way road (organization - audience).

b. the PR represent a "primary function of the management, based on a systematic and continuous activity, helping institutions find understanding, sympathy and support from those with whom they currently deal or will deal in the future"

Out of these definitions, one can identify the basic principles of any public relations activity; principles which are summed up in a few key words appeared in most definitions of the mentioned domain: leading position, ongoing conscious, planned and sustained effort, public interest, understanding, trust, bilateral communication, different kinds of audience.

Public relations may be included in two types of programs:

- Active offensive programs;
- Reactive programs which have a defensive character and consist of training specialists to deal with the unexpected and the inquiries received from various audiences.

Public relations can help organization deal with its image through the communication means serving best its interest avoiding all image crises the organization might face.

III.3. PUBLIC RELATIONS CAMPAIGNS

The most synthetic definition of public relations is given by R. Kendall: "the public relations campaign is a sustained effort of an organization to build reliable social relationships, in order to achieve certain objectives (determined after some research), effort based on the application of the communication strategies and the results evaluation"[8].

A public relations deployed plan can include programs, campaigns or events. An event takes place on a shorter and clearer period of time than a campaign or program; it covers only a goal and one or more well-defined audiences; the event may include punctual specific goals of reduced size.

The campaign is longer than the event, but they both have a well-defined beginning and an end. The campaign consists of a series of events or actions of public relations; the objectives are broader and involve more audiences.

The program differs from the other two terms by longer duration; also, it has no specific deadline; it is also made up of several events and public relations, he may continue as long as necessary and can even be periodically reviewed and adjusted, the goals are more extensive and concern general issues.

The PR campaigns can be classified according to several criteria. Considering the duration, they can be long and short, considering the content, they can target major themes or limited topics; considering the audience, they can be restricted to one type of public (internal audience), or may extend to all the organization's audiences; concerning the goals, they can be strategic or tactical.

The PR specialists experience shows that a successful campaign should sum up some characteristics:

- Defining needs, goals and public resources to target audiences;
- Systematic planning campaigns;
- Monitoring and continuous evaluation of the campaign;
- Selecting appropriate media for each type of audience

[8] Cristina Coman, *Relaţii publice- principii şi strategii*, Editura Polirom, Iaşi, 2001, pag.73

The campaign planning contains well-defined steps to follow, steps that come in a logical progression thus avoiding the waste of resources, time and money. The steps depend on one another and, each one resulting from the step taken before and leading the step to come.

A good campaign plan has to be consistent with the organization's goals and values, to be realistic (not to promise more than can be done), to be flexible, to reach values, interests and expectations of each target audiences.

Cristina Coman has synthesized various models from the specialized literature, she presents a campaign plan formula; this formula has the advantage that it can be applied to many types of campaigns: defining the problems, analyzing the situation, setting goals, identifying different audiences, establishing strategies and tactics, setting work schedule, budgeting, setting up evaluation procedures.

III.4. IMAGE CRISIS MANAGEMENT

A generally accepted definition of the crisis is that of an event (or series of events) which affects the product integrity, reputation or stability of the organization, the health or welfare of the employees, community or the general public. Crisis management involves the ability to anticipate crises, the development of any control and resolution scenarios, a quick response to the crisis, a firm discipline in compliance with the solution adopted, also the PR team and the officials of the organization.

According to Steven Fink, the development steps of the crisis are the following: - the preparation of the crisis, the acute phase, the chronic phase and the end of the crisis.

The image crisis can be defined as "that stage of deterioration of the notoriety, reputation and public confidence that endangers the functioning or existence of an organization"[9].

Several measures ought to be taken for the image crisis prevention:

- The organization's concern to create and manage a strong identity;
- The organization's total control over the messages visible in public places;
- To ensure a coherent, credible and stable image to the organization;
- Close coordination among the communication structures;

[9] Ion Chiciudean, *Gestionarea crizelor de imagine*, Editura SNSPA - Facultatea de Comunicare şi Relaţii Publice, Bucureşti, 2001, pag.75

- The creation of specialized structures in the image management area;
- A good management of the organizational crisis.

Although each image crisis is unique and requires different ways out, there are some common characteristics that must be taken into account:

- Deciding the parameters of the image to be projected on short, middle and long term;
- It does not appear suddenly, has a slow evolution influenced by the communicational environment;
- It overlaps is caused by a crisis of the organizational culture;
- It needs assessments and complex analyses;
- It has long-term effects;
- Affecting the credibility and reputation of the organization;
- The existence of the organization is in danger if nothing is done in order to restore the public image.

The communication of the crisis will be addressing: the actors of crisis, the internal and external audiences and the media. This last component is one of the most important ones. Experience has shown that often organizations are concerned with emergency measures and support less documentation work of journalists. In this case, journalists are resorting to rumors, or take a stand against organization, which brings further damage to its image.

We can say that crisis communication strategies aim to restore the image of the organization affected by the crisis.

Next I will present, briefly, two of the most popular models of such strategies. The first model belongs to W.L. Benoit who proposes the following Image Restoration Strategies:

a) The denial strategy is based on the denial of any involvement in the alleged facts;

b) The circumvention strategies consist in reducing the responsibility of the person or organization for the alleged facts and can take many forms: challenge, justification, accidental character, good intentions;

c) The strategies to reduce the dangerous character of the instruments by which, without circumventing the issue of liability, they are drawing attention that the facts are not so compromising and involve six directions: obtaining support, reduce negative feelings, differentiation, transcendence, attacking and compensation;

d) The strategies for correcting by which the accused person or organization move to correcting the damage done by two types of actions: restoration and promise;

e) The humiliation by which the accused person or organization plead guilty and ask publicly for forgiveness.

Another model belongs to W.T. Cobbs who proposes the following categories of crisis response strategies:

a) The denial strategies that aim to show that there is no crisis or that between the organization and crisis there is no cause-effect relation;

b) The distancing strategies, which acknowledge the crisis but try to weaken the links between crisis and organization in order to protect its image

c) The becoming friends strategies, aimed at winning public sympathy or approval for the organization by connecting it to those activities that are positively valued by the public;

d) The humiliation strategies, seeking to obtain public forgiveness and accept the conviction crisis;

e) The suffering strategies, which aim at winning public sympathy by assuming the pains caused by the crisis and by presenting the organization as a victim of unfavorable external conditions.

Finally allow me to present the main techniques for the image crisis resolution:

- Management of the organization's tools of communication;
- Minimization of the damage during the crisis;
- Reduction of the negative coverage in the press;
- Transformation of the crisis into opportunities;
- Ability to avoid staying a long time in the peak of the crisis;
- Capability to avoid open confrontation with the media;
- Promotion of the organization's new identity generated by the resolution of the organizational crisis"[10].

CONCLUSIONS

The brand is a particularly interesting area of study. A brand image can gradually substitute the reputation of an organization. Especially lately, we can speak about the "power of brand image" because, worldwide, brands are what people know

[10] Ion Chiciudean, *op.cit.,* pag.105

and buy, as consumers. When we say “know” we mean that people own good information about it. A well-known brand is, for instance, an assurance of the quality for the choice you make.

Our demanding modern life requires from every organization the duty to be present, transparent, active and generous in all aspects. Therefore, the public relations became that management function within the organization as important as other major management functions such as human resources, logistics and financial department and so on.

In fact, the public relations are visible everywhere. When the management of an organization requires from all employees a courteous, polite, caring behavior towards clients that develops a certain mood enabling relationships of sympathy with its audiences.

Thus, each person practices some form of public relations in the work he performs. When someone replies with a smile to a persistent glance or attempts to seduce by the intellectual qualities or personal charm, he/she seeks to create a sympathy relationship. Some people have a certain charisma; they can draw attention and sympathy naturally. Some personalities with these qualities mark the scene timeliness; others go without being noticed. When people or organizations do not naturally possess these forces of attraction, a certain sympathy background will help creating them. At that point the public relations will interfere, using a variety of professional techniques, trying to improve the situation.

In conclusion we can say that the brand image of an organization (or a person) is a patrimony object. Like a patrimony object, the image is managed and administered just like any other patrimonial good of the institution, regardless of its nature. A good image of the organization has a huge influence on its success and perception among the general public.

On the contrary, a negative image affects, sometimes in incredible manners, the success of the organization. To be effective, the image must evoke something, say something, has to invite to a possible dialogue. And all these problems can be best handled by the public relations using their specific methods.

REFERENCES

1. Coman, Cristina, *Relaţii publice - principii şi strategii*, Editura Polirom, Iaşi, 2001
2. Chiciudean, Ion, *Gestionarea crizelor de imagine,* Editura SNSPA - Facultatea de Comunicare şi Relaţii Publice, Bucureşti, 2001
3. Kotler, Philip, *Managementul marketingului*, Editura Teora, Bucureşti, 1997
4. Oprişan,Virginia,*Marketing şi comunicare în sport*, Editura Uranus, Bucureşti, 2002
5. Stancu, Valentin, *Relaţii publice - curs univ.*, Editura SNSPA - Facultatea de Comunicare şi Relaţii Publice, Bucureşti, 2001
6. Teodorescu, Bogdan, *Marketing politic şi electoral*, Editura SNSPA-Facultatea de Comunicare şi Relaţii Publice, Bucureşti, 2001

TRAINING AND LEARNING PLATFORM AT THE AIR FORCES APPLICATION SCHOOL FROM BOBOC

LTC Eng. Nelu DUMITRU

CONTENTS

TRAINING AND LEARNING PLATFORM AT THE AIR FORCES APPLICATION SCHOOL FROM BOBOC

INTRODUCTION

The “Aurel Vlaicu” Air Force Application School assures the initiation in career of the students (officers) who graduated "Henri Coandă" Air Force Academy and of those who were hired from external source (indirect career).

Air Force training and education programs are designed to develop well trained officers, enlisted and civilian personnel in the critical thinking skills and technical expertise demanded by today's military challenges. E-learning enhances traditional course development by blending the latest and best information and technology available with legacy systems and methods. Resident program curricula can be enhanced by reusing products developed and utilizing technology insertion in training and education programs.

The overall objective of the project is the development and modernization of the educational system in Air Force Application School "Aurel Vlaicu” through the implementation of an e-learning system allowing the creation of digital skills, access to courses online and off-line, with the help of information technology for active and collaborative participation of target beneficiaries.

Due to this development, graduates of the school of Air Force Application School "Aurel Vlaicu" will have a solid training that help them to perform in the knowledge society, in accordance with the requirements of condition the European market, thereby increasing economic competitiveness, the premise of productivity growth.

The specific objectives of the project are:

- production, presentation and update specific education curriculum within the air force
- reducing the time needed to develop teaching materials
- facilitating access to learning materials accessible to learners online
- facilitating access to teachers' tools for the creation of the electronic teaching material
- increase teacher training in the use of digital tools in education

These specific objectives will be achieved by carrying out several activities such as: development and implementation of an integrated information system for education by means of modern education; software and equipment acquisition necessary to support the solution implementation; digital content development required for implementation of the project; organizing of training courses for users and administrators of the system; information and publicity activities, according to the priorities of axis and major domain of intervention of the project.

I. GENERAL INFORMATION

I.1. Investment objective name & location

EDUCATIONAL TRAINING AND LEARNING PLATFORM AT THE AIR FORCES APPLICATION SCHOOL

Location

Place Boboc, Cochirleanca, Buzau

I.2. The holder of the investment

The holder of the investment is Air Forces Application School „Aurel Vlaicu".

I.3 The beneficiary of the investment (target groups)

The project aimed at implementing educational services online (eLearning) via a dedicated portal creates benefits for:

- 800 annual trainees of Air Forces Application School „Aurel Vlaicu"
- 70 teachers from Air Forces Application School „Aurel Vlaicu"
- At least 1.000 anual airforce specialist

II. GENERAL INFORMATION ABOUT PROJECT

II.1. Actual situation

II.1.1. AFAS objective

The MAIN OBJECTIVE of Air Forces Application School „Aurel Vlaicu" is the professional training of the officers, warrant officers and noncommissioned officers in accordance with the real need for development within the Air Force, for the

compliance, in its wholeness, with the standards, procedures and training and assessment technology of the armed force belonging to the other NATO member states, to accomplish, by structure, organization and content, the transformations and changes taking place in the Air Force.

OPERATIONAL OBJECTIVES**:**

- initial training for the first position of the Air Force Academy graduates;
- training of the Air Force officers, warrant officers and noncommissioned officers;
- planning, organizing and unfolding of courses for the professional military personnel;
- branch training of the professional soldiers within the Air Force;
- organizing the courses for the noncommissioned officers training (indirect branch);
- development of the personnel's foreign language knowledge level;
- organizing NATO specific military terminology courses and command and control military procedure training

SPECIFIC OBJECTIVES:

- adapting the military educational system to the new demands of the Air Force;
- organizing career and level courses ;
- managing the training courses for MIG-21 LanceR piloting;
- organizing the courses on time, especially concerning the level courses for S.C.C.A.N., air traffic control and Gap Filler;
- whole accomplishment of the training plan by the instructors;
- training within the English Language Secondary Learning Center, to obtain STANAG level;
- efficient use of the financial and material support needed for the training process;
- development of the command and control staff training;
- flight training for pilots;
- proper and permanent maintenance of the logistic support.

II.1.2. Actual IT systems

Information Resources Projects Completed

Some of the significant IR projects completed within the past two years are highlighted below:

- Significant advances have occurred in the data communications infrastructure. The Internal Building Wiring Project has been completed, resulting in the connection of all classrooms and offices to the local network, using fiber channel. Throughput has been increased via Gigabit Ethernet switching.
- The upgrade program has been completed; as a result AFAS have 4 modern labs and more than 300 workstations (Pentium dual core E6750, 1GB RAM, 250GB HDD, 17”LCD)
- Student transcripts can now be sent and received electronically.
- Two voice communications switched systems have been implemented to help air base operation. These system uses voice over IP

On-going Information Resources Initiatives

Work on several key projects identified within the previous years continues. The following paragraphs briefly describe some of the more wide-reaching projects currently under way:

- Technical support for students and staff end-users should continue to improve
- The e-mail system continues to grow; it currently services over 1000 accounts. Linux, which supports student e-mail among other functions, has been significantly expanded and enhanced.
- Wireless project will be finished until the end of this year. This system will provide wireless internet acces for 8 buildings.

II.1.3. Project management, personnel and training

Project management team:

- Project Manager
- Financial Responsible
- Technical Responsible
- Procurement Expert
- Legal expert

Project implementation methodology

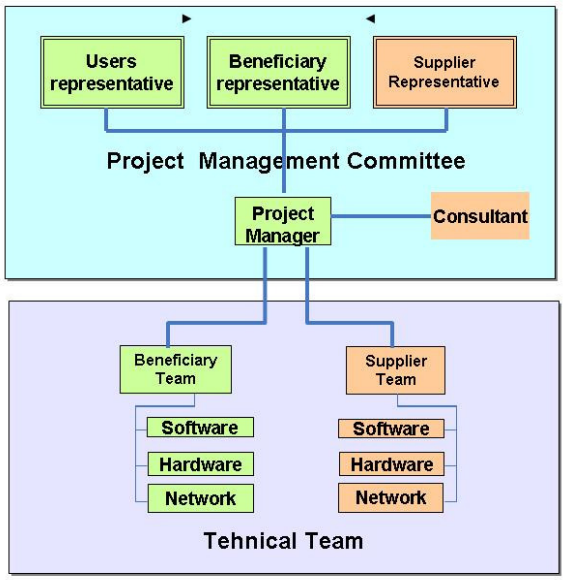
For the implementation of the project will use the method of planning and controlling phases of phases. Management team develops plan establishment and implementation of the project, setting the implementation phase with the responsibilities of each team member. Stage of activities is reviewed in monthly sessions for the analysis of the project, establishing measures of employment and compliance with deadlines laid down. During the sessions will be analyzed the risks and proposed measures for preventing and monitoring the implementation of the quality criteria.

Each activity will be conducted in compliance with the internal working procedures.

Project Organization and coordination strategy

The successful implementation of the project will be controlled at two levels:

- Project Management Committee
- Technical Team.



Products and services acquisition strategy

Having regarded to the fact that implementation of the proposed project involves and developing dedicated software solutions, the proposed acquisition strategy includes the implementation of a contract by a procedure of purchase in accordance with the legislation in force. This contract is required for the selection of specialized company providing information technology solution (hardware and software) with which to be able to achieve the project objectives. It will hold a single procedure for the award of a "supply of Goods", respecting the procedures imposed

by the funder. Within this auction, will have the role of contracting authority and will prepare the necessary documentation for the selection of a company with the role of "integrator". "Integrator" company will have to suply all the technical equipment provided for in standard software applications, but also to develop specialized eLearning application. "Integrator" company will configure, install and give up all equipment and software necessary, but will ensure and maintain such equipment for a period of 5 years after the completion of the project.

In terms of the acquisition strategy, the benefits of the proposed strategy are multiple:

- Minimizing administrative and logistical tasks and avoidance of multiple acquisition processes, by purchasing all supplies from a "integrator" company.
- Minimizing technical risk by selecting a company with specialized experience in the implementation of similar systems.
- Minimizing the risk of insufficient human resources in specialized, by transferring technical liability by the "integrator"company.
- Avoiding risk of technological integration of equipment and applications purchased by purchasing all supplies from a single source.
- Obtaining a guarantee unique to the entire integrated system, what makes long-term investment protection.

Project management activities

Project management activities relate to project management methodology.

Project Management Plan is based on a number of other plans, in the structure identified below:

<table>
<tr><th colspan="6">Project Management Plan</th></tr>
<tr><td colspan="6">Specific plans</td></tr>
<tr><td>Setup Plan</td><td>Quality Plan</td><td>Communica-tion Plan</td><td>Risck Management Plan</td><td>Resourses Plan</td><td>Implementation Plan</td></tr>
<tr><td>Accep-tance Plan</td><td>Trainin g Plan</td><td>Infrastructure Installation Plan</td><td>Application Integration Plan</td><td>Warranty Plan</td><td>Maintenance Plan</td></tr>
</table>

These plans are dynamic and will evolve during the project. Plans that identify the progress of project activities will be presented at the Committee meetings for the

evaluation of the project and will be kept by the project manager in accordance with the Change Management Procedure.

The list of these plans, as well as their maintenance responsibility, is shown in the table below:

Plan	**Responsible**
Quality Plan	Project Manager
Communication Plan	Project Manager
Risck Management Plan	Project Manager
Resourses Plan	Project Manager
Setup Plan	Project Manager, Project Manager
Implementation Plan	Supplier Representative, Project Manager
Application Integration Plan	Supplier Representative, Project Manager
Acceptance Plan	Project Manager, Supplier Representative
Training Plan	Supplier Representative, Project Manager
Infrastructure Installation Plan	Supplier Representative, Project Manager
Warranty Plan	Supplier Representative, Project Manager
Maintenance Plan	Supplier Representative, Project Manager

The methodology used will include:

Organizing project

- Establish guidelines of the project.
- Project team management.
- Achievement of livrabilelor project.

Project planning

- Deliverables Planning.
- Planning activities necessary for the attainment of these deliverables.
- Planning activities necessary for validation of the quality of these deliverables.
- Planning resources and time necessary for the realization of activities (including quality control activities), as well as the identification of specialized resources necessary.
- Defining the links and dependencies between activities.

- Defining of possible external dependencies on the provision of information, products or services.
- Defining moments in time when various activities will be held.
- Establish control points when will be monitoring progress.

Project control

- Pogress monitoring
- Initiation of corrective measures.

Risk management

- identification of risks that may affect the project.
- The risk estimation- determination of the importance of each risk on the basis of an assessment of its consequences on the project.
- Risk assessment, action to decide whether the risk is acceptable, and if not, then it will decide what action should be taken to bring the level of the risk to an acceptable level.
- Resource allocation – consists in identifying and allocating the resources that will be used to act in order to avoid risk or minimize its impact; these appropriations will be included in the plan Stage; the necessary resources for undertaking actions for the prevention, reduction and transfer will be borne by the budget of the project.
- Monitoring –verifying that the actions planned and implemented have the desired effect on the risks identified; examining the early signals of risk; forecasting the potential risks; Verify that risk management is carried out in an efficient manner.
- Control – actions to be taken and by which to verify that the plans are respected.

Quality management

- Quality plan.
- Monitoring the implementation of the quality criteria with respect to functional performance requirements: security, compatibility, safety, ease of maintenance, flexibility, possibility of extension, the clarity, the comparison with another product, cost, time required for implementation.

Configurations Management

- Planning – decision on the level of required configuration management project and determining how this level will be achieved.
- Identification – identifies and specifies all components livrabilului.
- Control – the ability to approve and then to "freeze" a particular deliverable and then to make changes upon himself only with the approval of an authority clearly established.
- Condition Management – recording and reporting of all current and historical data related to the evolution of a deliverable.
- Check – series of checks and audits to ensure that there is conformity between the product and the condition of the product, as it is recorded in the Register of Deliverables Configurations.

Change control

- Evaluation of the impact of a potential change can produce priority, cost and an eventual decision on the implementation of management change.
- Request for change of specifications.
- Suggestion to improve one or more deliverables from the project.

Monitoring the implementation of the project

Monitoring will be accomplished by the project manager of the applicant, through a series of main means of control available to the Steering Committee of the project:

- Checking the End of Stage (has been successfully finished the preceding stage? The project is carried out in accordance with the Project Plan? The economic justification of the project is still viable? The risks are under control? You can move to a new phase?).
- Status reports (regular Reports during a stage).
- Exception reports (Advance Notification on forecasts of deviation from approved tolerance limits).
- Intermediate Verification stage (the Management Committee of the project examines and decides what position to adopt in response to a report by exception).
- Closing the project (the project has delivered everything they had? Additional activities are needed? What are the conclusions following the progress of the project?).

Evaluation of the results of the project is the process by which information is obtained on the quality of the project, measuring the results in relation to objectives in order to take strategic decisions to support implementation and project management. It will be accomplish both ongoing assessment and the final assessment, according to the scheme of assessment. Ongoing assessment, carried out during the life of the project will be focused on the following aspects:

- allotted time;
- assigned budget;
- the effects of the implementation of the project for the institution;
- cooperation among project team members.

The final assessment will be achieved at the end of the period of implementation of the project, at which point all of the components of the project (process, relevance and consistency of the measures taken, the activities, added value) will be taken into account in order to examine the results. The evaluation will be both quantitative and qualitative and will concern:

- The resources invested;
- Activities carried out;
- Results obtained;
- Achieving the performance levels proposed in the planning;
- Changes and their consequences;
- Effects of implementation for institution;
- Level of local ownership of project results.

In the interests of effective and impartial analyses will be conducted and an external evaluation, ordered to avoid the disadvantages of using a single type of evaluation, often subjective, namely that of internal evaluation.

Staff and training

Staff

The applicant's project team consists of three people with complementary competences:

Project Manager (PM)

- Ensure the overall conduct of the project team in order to attain its objectives and compliance with deadlines laid down;

- Ensures the management of the relationship with the financier, as well as with other third parties involved in the project,
- Contribute to preparing the specifications for carrying out procurement procedures
- Prepares activity reports for the Financier by centralising reported the other members of the project team
- Check/monitor the contractor's activity that will provide project management services
- Resolve conflicts and takes care that they do not impede the smooth functioning of the project;
- Resolves issues that may arise as unanticipated situations, including by requiring some amendments to the conditions of the contract;
- Assess the results of implementation of the project permanently according to the schedule of activities approved and ensures continuous and smooth scrolling to carry out the activities;
- Coordinates and monitors the performance of the obligations of information and publicity for the project according to the requirements of the contract financing

Financially Responsible (FR)

- Reports to the project manager and Consultant specializing in collaborating with the conduct of the procedures for purchases and payments • is responsible for the coordination of activities in regard to organizing procedures of purchase and subsequent execution of contracts signed with select suppliers;
- Coordinates and monitors the implementation of contracts • coordinates and monitors the preparation of applications for reimbursement by the financier, assisted by the contractor which will provide project management services ensures the management of bank accounts opened for operation of financial transactions related to the implementation of the project;
- Ensures that the cost of the project, separate accounting records and transparent implementation of the project;
- Provide and be responsible for the smooth operation of financial accounting activities and preparation of specific documents for making disbursements and are contracting firms and with the Contracting utoritatea and sheep;

- Verifies the eligibility of the expenditure sent for settlement;
- Proposing corrective solutions in case of referral of disfunctionalităţi in implementation of the project;
- Ensure documentation and organizing computer files in a manner allowing their keeping for a period of five years after the official closure POSCCE (2017) and the possibility of accessing them in optimal conditions by the bodies empowered to verify or to carry out the audit of the implementation of the project.

Technical responsible

- Reports to the project manager
- Ensures intake of technical knowledge necessary for drawing up the specifications and equipment suitable for the election, as well as the contribution required in the other phases of the project.
- It coordinates the technical team that will ensure the monitoring operations hardware, software, network equipment, installing applications, hardware and software configurations.

Training

- courses for end users: these relate to the use of the new system implemented;
- courses for system administrators: they refer to the system administration, database administration, user support, infrastructure management hardware.

For each category of courses the provider will present: course description, target audience, the course structure, the minimum knowledge requirements which must be met by learners, course duration.

Requirements for training courses

- Courses of Administration (database, HW infrastructure) will be provided by instructors;
- For each course will be provided by the course manuals;
- Each student will receive at the end of each certified training course

Conduct training

The training will take place on-site at the faculty, according to the plan of instruction set and agreed contractually. Training will keep the Roman language, using interactive methods combined with classical methods, by instructors from imagination project. The recipient will provide the hardware and software

infrastructure. The training will be done on the basis of the French course, delivered by each participant's project will produce. This course will contain practical examples for a better understanding of the functioning and administration of the system, as well as other details related to it.

User training will be done on a test environment that will use a test database.

Manuals and documentation

Will be provided the following manuals and documentation: • technical documentation of equipment and basic software, supplied by a producer;

- manual installation and configuration of the equipment and software;
- system administration manuals/solution;
- manuals for system components/solution;
- functional documentation system/components of the solution;
- technical documentation system/components of the solution;
- other manuals/documentation set in the aftermath of the period of analysis;

Will be provided all the manuals and documentation in the Romanian language, with the exception of technical documentation of equipment and basic software, provided by the manufacturers, who may be in English.

Manuals and documentation will be delivered on paper and electronic media (CD, DVD) and will be reviewed at every change of the software version.

II.2. Investment Description

II.2.1. The current situation, the necessity and oportunity of promoting investment

Proposed project is justified by the need to align Air Forces Application School „Aurel Vlaicu" to standards, procedures, training and evaluation technologies of NATO Alliance, adaptation of educational and training processes to new requirements and realities of the air force, the preparation of new coursesincluding preparation of instructors and the necessary material base, and effective use of financial and material resources required for training and education.

ELearning systems at Air Forces Application School „Aurel Vlaicu" needs are:

- creation of easily accessible training system – each user has access to it from the computer that works;

- ensuring a uniform and comprehensive understanding of the topics of learning;
- providing of homogeneous course materials – the same course materials for the specific theme;
- decrease the time taken for the process of training/instruction per user
- lowering costs (financial and material) required for learning/training
- continuous providing to the training/information of all learners;
- building an electronic database containing relevant documents for each student;
- providing of automated assessment tools;
- providing of content creation tools.

Thus, the advantages of implementing an e-learning system are those that allow the learners familiarity with IT, has the ability to make available to the student more learning resources, enabling linking them with a global educational community. Due to the use of an e-learning platform with powerful functions of LMS (Learning Management System), planning course is much more effective, the material is centred on the student and on the level of knowledge, real time access to the knowledge anywhere and anytime without involving travel expenses often interrupting current professional activity.

II.2.2. Technical-economic scenarios through which investment project objectives can be achieved and chosen scenario benefits

Technical-economic scenarios considered are those based on:

Variant 1 – use of WEB technology

To ensure the intended purpose through a project implementing SW version is integrated with the main modules: portal and eLearning application.

In this version of the proposal is to be a single portal and a single application of eLearning in the Web technology which ensure:

- anywhere access of users through the web browser;
- controlled access with authentication;
- learners centralized monitoring and reporting;
- reduced costs of maintenance and administration;
- implementation of a security mechanism.

Variant 2 – Using client-server technology

This variant will use technical access to the server with downloading content on local stations and ensure:

- users' access to the server based authentication
- downloading content on client computer
- deploy a powerful security mechanism

II.2.3. Functional and technical description

Functional architecture of the system

The project described in this document follows the development and modernization of the educational system within the Air Forces Application School "Aurel Vlaicu" through the creation of digital skills, use of information technology and communication for knowledge and problem solving, for active participation in collaborative projects, scientific research group of target beneficiaries.

Integrated computer system proposed in this project will provide the following capabilities:

- Integrated Functionality at the portal level based on web technology;
- Ensure a centralized secure access for beneficiaries of services offered (teachers, students, doctoral students, researchers, etc.);
- Creation of a safe and effective tool for managing courses, tests, psychological research online in the faculty, to streamline internal activities and interaction with beneficiaries of services offered;
- Ensuring a stable and secure electronic environment of interaction;
- Creation of technical means for providing information needed to optimize procedures.

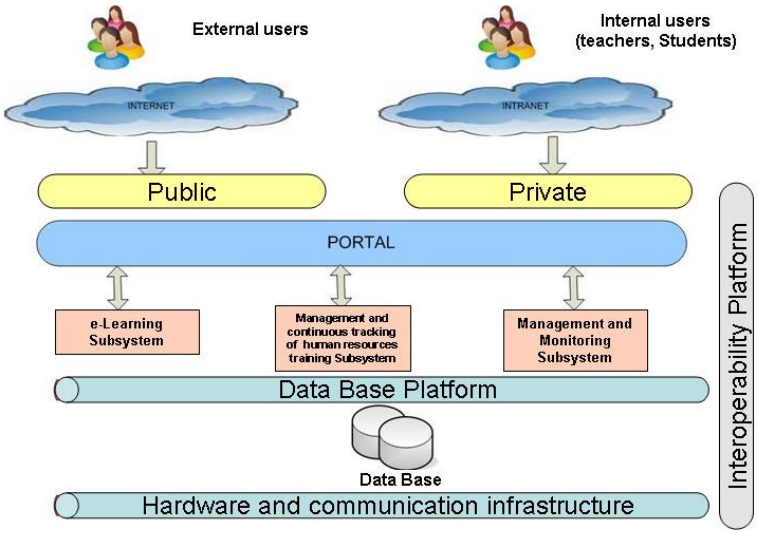
Integrated computer system that will be implemented will be based on a services-oriented architecture (SOA-Oriented Architecture Services, within the meaning of the definition and meaning of the OASIS Consortium – the Organization for the Advancement of Structured Information Standards), with maximum flexibility in integration with other systems and the changes that can occur in the informational flows of system processes.

The system will be accessible and can be used by a large number of users, without the need of advanced knowledge in terms of software applications.

The computer system will ensure, for all modules, a high degree of availability by ensuring redundancy both in hardware and software ("no single point of failure").

The services provided by the system will be implemented on a specialized platform for execution of business processes, and interface for access to these services will be designed as an intuitive portal, with easy to learn. Navigating between components of the system will be intuitive, based on a high ergonomics so that, where possible, to make predefined screens sequences for certain activities available to the user.

The following figure shows the functional architecture of the system, with users identification, user interface, and applications structure.



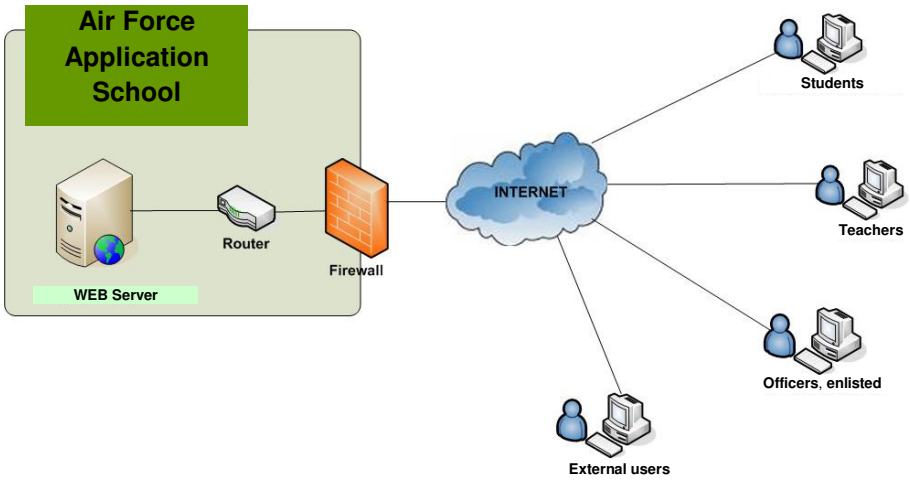
Functional System Architecture

From the technical point of view, the functional system components will by support on certain technical components: server applications, database management system data, hardware and communication infrastructure.

Technical design of integrated computer system is based on the following premises:

- User Interface is web browser – the application is web based;
- The architecture of web applications is n-tier;
- Online services Portal is available to all categories of users.

Technical web application architecture is shown below:



Technical web application architecture

N-tier architecture

All software will be built according to the principles web multitier architecture over the next logical levels clearly separated:

- Presentation level - the user interface will provide a service menu with the possibility of navigation between options and sub options. The UI will be intuitive (easy), informative, reliable, attractive and stable.
- The logical business model level - business logic ensures transparency of the complexity of its users, being organized according to the following principles:
    - Standardization.
    - Re-use.
    - Clear separation between the presentation and business logic

Business logic level provides handling all processing rules including:

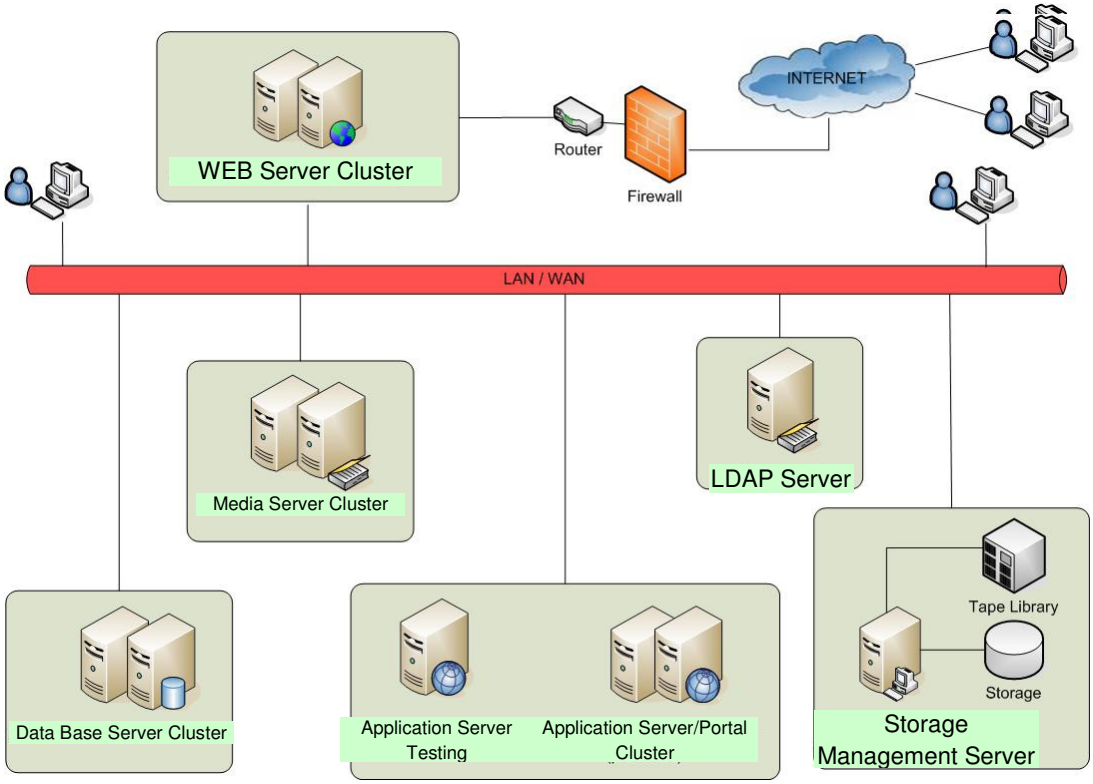
- Authentication and security authorization.
- Users sessions management.
- Data integrity rules.
- Validation rules entries.
- Monitoring transactions.
- Information and data.

Information stored in databases and used within the application has the following features:

- large volume of information collected from existing sources.
- heterogeneous data sources (databases, data entered via the portal, existing applications).
- high accuracy, obtained by checking the input sources, reporting any discrepancies.
- the need to support a process of complex analysis, the necessary information flow within the school.

In this architecture, the solution proposed will make available to internal and external users, according to access rights held, a common access point (portal) to information managed by different modules.

The technical architecture of the system is shown in the figure below:



System technical architecture

The following quantitative elements will be taken into account in assessing the proposed solution:

- The number of users of the system.
- The response time of the services accessible via the portal.
- The number of referrals of online services offered through the portal.

II.3. Technical data of the investment (taken from the technical project attached to the feasibility study)

Training and learning platform that we want to be implemented within the Air Forces Application School „Aurel Vlaicu" will be a modular, easily expandable, consisted of the following components:

- **The Portal subsystem –** this component will integrate all applications (system components) and will be the common interface for working with learners, teachers, other institutions will have access depending on the assigned role; The portal will include private area (only accessible to users who have access to the system account), the public area (accessible to the general public for consultation of useful information) and email client integration;
- **E-Learning subsystem –** this subsystem will include 2 components: e-Learning (auto-training, testing, virtual classes) and e-Content (content development);
- **Management and continuous tracking of human resources training subsystem –** this component will enable all trainees management to ensure the regularity of participation in continuing training courses;
- **Management and monitoring subsystem** – this component will manage the administration and monitoring of hardware and communication infrastructure of the system;
- **Data management system** – this is a modul that asure secure data storage in the form of a relational database , with extensive replication and backup capabilities;
- **Hardware component** – hardware infrastructure ensures necessary for optimum running of the subsystems that make up "educational platform for training and learning at the Air Forces Application School";
- **Communications component** – ensures the necessary communications infrastructure.

III. ESTIMATED COST OF THE INVESTMENT

The staggering costs in conjunction with the implementation of the investment.

Index	Activity	Responsabil	De la	Până la	Costs
1	**Solution Implementation**		Day 1, Month 6	Day 30, Month 21	
1.1	System needs analysis	Project manager, Provider IT representative	Day 1, Month 6	Day 30, Month 8	329,000.00
1.2	Delivery of hardware equipment and software licenses and installation	Technical Responsible, Project manager, Provider IT representative	Day 1, Month 9	Day 1, Month 10	2,288,398.12
1.3	Development and installation of the eLearning platform	Technical Responsible, Project manager, Provider IT representative	Day 1, Month 8	Day 30, Month 12	584,723.32
1.4.	Development and installation of Managing and tracking continuous training of human resources Subsystem	Technical Responsible, Project manager, Provider IT representative	Day 1, Month 8	Day 30, Month 12	306,400.00
1.5.	Testing the solution	Technical Responsible, Project manager, Provider IT representative	Day 1, Month 13	Day 30, Month 14	38,700.00
1.6.	Online electronic teaching materials/online courses elaboration	Technical Responsible, Project manager, Provider IT representative	Day 1, Month 15	Day 30, Month 19	673,075.68

Index	Activity	Responsabil	De la	Până la	Costs
1.7.	The Pilot and release for use	Technical Responsible, Project manager, Provider IT representative	Day 1,Month 19	Day 1, Month 21	90,300.00
				TOTAL	**4,310,597.12**

Conclusions

Considering the two functional alternatives identified, we prefer version 1 because it can fulfill the functionalities identified by beneficiary through the requirements expressed and presents lower cost because it does not involve additional installation on the client machines.

Implementation of client-server type (Variant 2) brings with it a technological constraint where users number is large enough (over 100 users), given the requirement for all users to connect remotely on the server machine. The solution proposed in Variant 2 can generate security problems.

REFERENCES

1. Ministry of Communications and Information Society - *The applicant's Guide for 3 operation "Support the implementation of E-Education applications"*
2. Air Force Application Scool - *Educational training and learning platform at the Air Forces Application School- feasibility study*
3. *http://fonduri.mcsi.ro/?q=node/75*.

BENEFITS AND RECOMMENDATIONS FOR INFORMATION SECURITY IN CLOUD COMPUTING

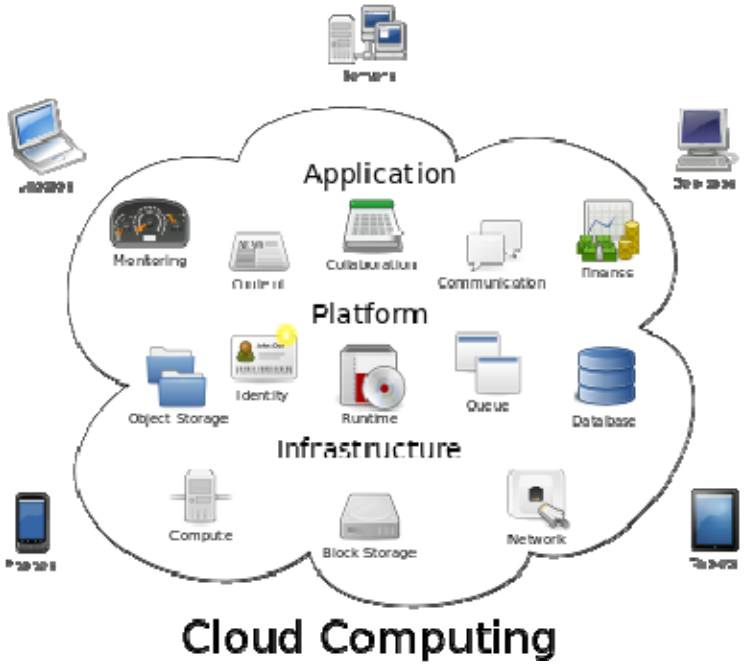
Capt. cmdr. Valeriu ANTON

CONTENTS

BENEFITS AND RECOMMENDATIONS FOR INFORMATION SECURITY IN CLOUD COMPUTING

INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.



In the business model using software as a service users also rent application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run.

End users access cloud-based applications through a web browser or a light-weight desktop or mobile while the business software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.

Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

I. HISTORY

The origin of the term cloud computing is obscure, but it appears to derive from the practice of using drawings of stylized clouds to denote networks in diagrams of computing and communications systems. The word cloud is used as a metaphor for the Internet, based on the standardized use of a cloud-like shape to denote a network on telephony schematics and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents. The cloud symbol was used to represent the Internet as early as 1994.

The underlying concept of cloud computing dates back to the 1950s; when large-scale mainframe became available in academia and corporations, accessible via thin clients / terminal computers. Because it was costly to buy a mainframe, it became important to find ways to get the greatest return on the investment in them, allowing multiple users to share both the physical access to the computer from multiple terminals as well as to share the CPU (central processing unit) time, eliminating periods of inactivity, which became known in the industry as time-sharing.

John McCarthy opined in the 1960s that "computation may someday be organized as a public utility." Almost all the modern-day characteristics of cloud computing (elastic provision, provided as a utility, online, illusion of infinite supply), the comparison to the electricity industry and the use of public, private, government, and community forms, were thoroughly explored in Douglas Parkhill's 1966 book, “The Challenge of the Computer Utility”. The development of the Internet from being document centric via semantic data towards more and more services was described as "Dynamic Web". This contribution focused in particular in the need for better meta-data able to describe not only implementation details but also conceptual details of model-based applications.

The availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, autonomic, and utility computing have led to a tremendous growth in cloud computing.

Amazon played a key role in the development of cloud computing by modernizing their data centers, which, like most computer networks, were using as little as 10% of their capacity at any one time, just to leave room for occasional spikes. Having found that the new cloud architecture resulted in significant internal efficiency improvements whereby small, fast-moving "two-pizza teams" (teams small enough to be fed with two pizzas) could add new features faster and more easily, Amazon initiated a new product development effort to provide cloud computing to external customers, and launched Amazon Web Service (AWS) on a utility computing basis in 2006.

In early 2008, Eucalyptus became the first open-source, AWS API-compatible platform for deploying private clouds. In the same year, efforts were focused on providing quality of service guarantees (as required by real-time interactive applications) to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, resulting to a real-time cloud environment. By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them"[1] and observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models" so that the "projected shift to computing... will result in dramatic growth in IT products in some areas and significant reductions in other areas."[2]

On March 1, 2011, IBM announced the Smarter Computing framework to support Smarter Planet. Among the various components of the Smarter Computing foundation, cloud computing is a critical piece.

II. CHARACTERISTICS

Cloud computing exhibits the following key characteristics:

- **Agility** improves with users' ability to re-provision technological infrastructure resources.
- **Application programming interface (API)** accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers.
- **Cost** is claimed to be reduced and **in a public cloud** delivery model **capital expenditure** is converted to **operational expenditure**. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state of the art repository [3] contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.
- **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
- **Virtualization** technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.
- **Multitenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
    - Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
    - Peak-load capacity increases (users need not engineer for highest possible load-levels)
    - Utilization and efficiency improvements for systems that are often only 10–20% utilized.[4]
- **Reliability** is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- **Scalability and elasticity** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.
- **Performance is monitored** and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Security could improve** due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible.

Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

- **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

II.1. On-demand self-service

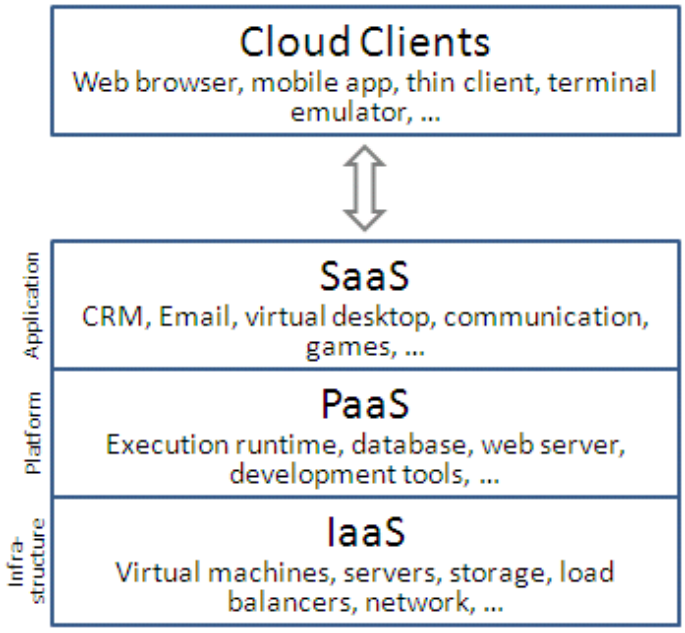
On-demand self-service allows users to obtain, configure and deploy cloud services themselves using cloud service catalogues, without requiring the assistance of IT. This feature is listed by the National Institute of Standards and Technology (NIST) as a characteristic of cloud computing.

The self-service requirement of cloud computing prompts infrastructure vendors to create cloud computing templates, which are obtained from cloud service catalogues. Manufacturers of such templates or blueprints include Hewlett-Packard (HP), which names its templates as HP Cloud Maps, RightScale and Red Hat, which names its templates CloudForms.

The templates contain predefined configurations used to by consumers to set up cloud services. The templates or blueprints provide the technical information necessary to build ready-to-use clouds. Each template includes specific configuration details for different cloud infrastructures, with information about servers for specific tasks such as hosting applications, databases, websites and so on. The templates also include predefined Web service, the operating system, the database, security configurations and load balancing.

III. SERVICE MODELS

Cloud computing providers offer their services according to three fundamental models: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models.



III.1. Infrastructure as a service (IaaS)

In this most basic cloud service model, cloud providers offer computers, as physical or more often as virtual machines, and other resources such file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. For wide area connectivity, the Internet can be used or—in carrier clouds -- dedicated virtual private networks can be configured., To deploy their applications, cloud users then install operating system images on the machines as well as their application software. In this model, it is the cloud user who is responsible for patching and maintaining the operating systems and application software. Cloud providers typically bill IaaS services on a utility computing basis, that is, cost will reflect the amount of resources allocated and consumed.

IaaS refers not to a machine that does all the work, but simply to a facility given to businesses that offers users the leverage of extra storage space in servers and data centers.

Examples of IaaS include: Amazon CloudFormation (and underlying services such as Amazon EC2), Rackspace Cloud, Terremark, Windows Azure Virtual Machines, Google Compute Engine and Joyent.

III. 2. Platform as a service (PaaS)

In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying computer and storage resources scale automatically to match application demand such that cloud user does not have to allocate resources manually.

Examples of PaaS include: Amazon Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard, Mendix, Google App Engine, Windows Azure Compute and OrangeScape.

III.3.Software as a service (SaaS)

In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its scalability. This can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be multitenant, that is, any machine serves more than one cloud user organization. It is common to refer to special types of cloud based application software with a similar naming convention: desktop as a service, business process as a service, test environment as a service, communication as a service.

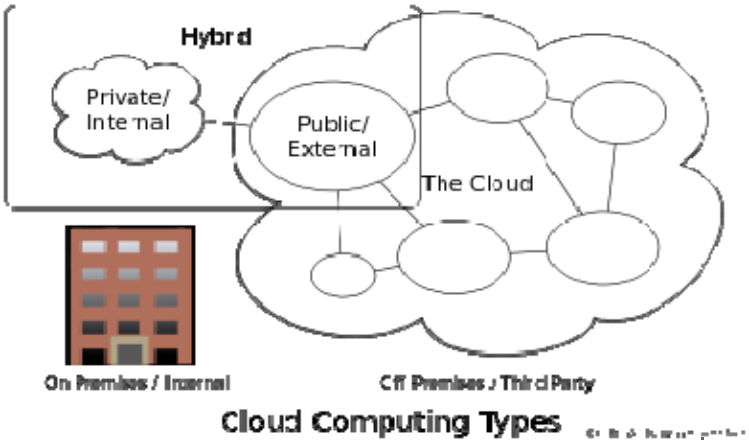
The pricing model for SaaS applications is typically a monthly or yearly flat fee per user, so price is scalable and adjustable if users are added or removed at any point.

Examples of SaaS include: Google Apps, Microsoft Office 365, and Onlive.

IV. CLOUD CLIENTS

Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and smartphones. Some of these devices - *cloud clients* - rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application.

V. DEPLOYMENT MODELS



Cloud Computing Types

V.1. Public cloud

Public cloud applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access only via Internet (direct connectivity is not offered).

V.2.Community cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

V.3 Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity.

V.4. Private Cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and it will require the organization to reevaluate decisions about existing resources. When it is done right, it can have a positive impact on a business, but every one of the steps in the project raises security issues that must be addressed in order to avoid serious vulnerabilities.

VI. SECURITY BENEFITS OF CLOUD COMPUTING

Cloud computing has significant potential to improve security and resilience. What follows is a description of the key ways in which it can contribute.

VI.1. Security and the benefits of scale

Put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, human resources and their management and vetting, hardware and software redundancy, strong authentication, efficient role-based access control and federated identity management solutions by default, which also improves the network effects of collaboration among various partners involved in defense. Other benefits of scale include:

- **Multiple locations**: most cloud providers have the economic resources to replicate content in multiple locations by default. This increases redundancy and independence from failure and provides a level of disaster recovery out-of-the-box.
- **Improved timeliness of response**: larger **to incidents**: well-run larger-scale systems, for example due to early detection of new malware deployments, can develop more effective and efficient incident response capabilities.
- **Threat management**: cloud providers can also afford to hire specialists in dealing with specific security threats, while smaller companies can only afford a small number of generalists.

VI. 2. Security as a market differentiator

Security is a priority concern for many cloud customers. Customers will make buying choices on the basis of the reputation for confidentiality, integrity and resilience, and the security services offered by a provider, more so than in traditional environments. This is a strong driver for cloud providers to improve their security practices and compete on security.

VI.3. Standardized interfaces for managed security services

Large cloud providers can offer a standardized, open interface to managed security services (MSS) providers offering services to all its customers. This potentially creates a more open and readily available market for security services where customers can switch providers more easily and with lower set-up costs.

VI.4. Rapid, smart scaling of resources

The list of cloud resources which can be rapidly scaled on demand already includes, e.g., storage, CPU time, memory, web service requests and virtual machine instances, and the level of granular control over resource consumption is increasing as technologies mature.

A cloud provider has the potential to dynamically reallocate resources for filtering, traffic shaping, encryption, etc, in order to increase support for defensive measures (e.g., against DDoS attacks) when an attack is likely or it is taking place.

VI.5. Audit and evidence-gathering

IaaS offerings support on-demand cloning of virtual machines. In the event of a suspected security breach, the customer can take an image of a live virtual

machine – or virtual components – for offline forensic analysis, leading to less down-time for analysis. This improves the ex-post analysis of security incidents and increases the probability of tracking attackers and patching weaknesses.

It can also provide more cost-effective storage for logs, thus allowing more comprehensive logging without compromising performance.

VI.6. More timely and effective updates and defaults

Virtual machine images and software modules used by customers can be pre-hardened and updated with the latest patches and security settings according to fine-tuned processes. Updates can be rolled out many times more rapidly across a homogenous platform than in traditional client-based systems that rely on the patching model.

VI.7. Benefits of resource concentration

Although the concentration of resources undoubtedly has disadvantages for security, it has the obvious advantage of cheaper physical perimeterisation and physical access control (per unit resource) and the easier and cheaper application of a comprehensive security policy and control over data management, patch management, incident management, and maintenance processes.

VII. INFORMATION ASSURANCE REQUIREMENTS

VII.1. Personnel security

The majority of questions relating to personnel will be similar to those it would ask to the IT personnel or other personnel who are dealing with IT. As with most assessments, there is a balance between the risks and the cost.

- What policies and procedures do you have in place when hiring your IT administrators or others with system access? These should include pre-employment checks (identity, nationality or status, employment history and references, criminal convictions etc.).
- Are there different policies depending on where the data is stored or applications are run?
  - For example, hiring policies in one region may be different from those in another.
  - Practices need to be consistent across regions.
  - It may be that sensitive data is stored in one particular region with appropriate personnel.
- What security education program do you run for all staff?
- Is there a process of continuous evaluation?

VII.2. Operational security

It is expected that any commercial agreement with external providers will include service levels for all network services. However, in addition to the defined agreements, the end customer should still ensure that the provider employs appropriate controls to mitigate unauthorized disclosure.

- Detail your change control procedure and policy. This should also include the process used to re-assess risks as a result of changes and clarify whether the outputs are available to end customers.
- Define the remote access policy.
- Does the provider maintain documented operating procedures for information systems?
- Is there a staged environment to reduce risk, e.g., development, test and operational environments, and are they separated?

- Specify the controls used to protect against malicious code.
- Are secure configurations deployed to only allow the execution of authorized mobile code and authorized functionality (e.g., only execute specific commands)?
- Detail policies and procedures for backup. This should include procedures for the management of removable media and methods for securely destroying media no longer required.
- Can the provider detail what information is recorded within audit logs?
- For what period is this data retained?
- What controls are employed to protect logs from unauthorized access or tampering?
- What method is used to check and protect the integrity of audit logs?

VII.2.1. Software assurance

- Define controls used to protect the integrity of the operating system and applications software used.
- How do you validate that new releases are fit-for-purpose or do not have risks (backdoors, Trojans, etc)? Are these reviewed before use?
- What practices are followed to keep the applications safe?
- Is a software release penetration tested to ensure it does not contain vulnerabilities? If vulnerabilities are discovered, what is the process for remedying these?

VII.2.2. Network architecture controls

- Define the controls used to mitigate DDoS (distributed denial–of-service) attacks.
  - Defense in depth (deep packet analysis, traffic throttling, packet black-holing, etc)
  - Do you have defenses against 'internal' (originating from the cloud providers networks) attacks as well as external (originating from the Internet or customer networks) attacks?
- What levels of isolation are used for virtual machines, physical machines, network, storage (e.g., storage area networks), management networks and management support systems, etc.?
- Does the architecture support continued operation from the cloud when the company is separated from the service provider and vice versa ?
- Is the virtual network infrastructure used by cloud providers secured to vendor and/or best practice specific standards?

VII.2.3. PAAS – Application security

Generally speaking, PaaS service providers are responsible for the security of the platform software stack. It is often difficult to obtain detailed information from PaaS providers on exactly how they secure their platforms – however the following questions, should be of assistance in assessing their offerings.

- What assurance can the PaaS provider give that access to your data is restricted to your enterprise users and to the applications you own?
- The platform architecture should be classic 'sandbox' – does the provider ensure that the PaaS platform sandbox is monitored for new bugs and vulnerabilities?
- PaaS providers should be able to offer a set of security features (re-useable amongst their clients) – do these include user authentication, single sign on, authorization (privilege management), and SSL/TLS (made available via an API)?

VII.2.4. SAAS – Application security

The SaaS model dictates that the provider manages the entire amount of applications delivered to end-users. Therefore SaaS providers are mainly responsible for securing these applications. Customers are normally responsible for operational security processes (user and access management). However the following questions should assist in assessing their offerings:

- What administration controls are provided and can these is used to assign read and write privileges to other users?
- Is the SaaS access control fine grained and can it be customized to your organizations policy?

VII.2.5. Resource provisioning

- In the event of resource overload (processing, memory, storage, network)?
  - What information is given about the relative priority assigned to my request in the event of a failure in provisioning?
  - Is there a lead time on service levels and changes in requirements?
- How much can you scale up? Does the provider offer guarantees on maximum available resources within a minimum period?
- How fast can you scale up? Does the provider offer guarantees on the availability of supplementary resources within a minimum period?

VII.3. Identity and access management

The following controls apply to the cloud provider's identity and access management systems (those under their control):

VII.3.1. Authorization

- Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations (read/write/delete)?
- How are the accounts with the highest level of privilege authenticated and managed?
- Are any high-privilege roles allocated to the same person? Does this allocation break the segregation of duties or least privilege rules?
- What changes, if any, are made to administrator privileges and roles to allow for extraordinary access in the event of an emergency?
- Is there an 'administrator' role for the customer? For example, does the customer administrator have a role in adding new users ?

VII.3.2. Management of personal data

- What data storage and protection controls apply to the user directory and access to it?
- Is user directory data exportable in an interoperable format?
- Is need-to-know the basis for access to customer data within the cloud provider?

VII.3.3. Key management

For keys under the control of the cloud provider:

- Are security controls in place for reading and writing those keys? For example, strong password policies, keys stored in a separate system, hardware security modules (HSM) for root certificate keys, smart card based authentication, direct shielded access to storage, short key lifetime, etc.
- Are security controls in place for using those keys to sign and encrypt data?

- Are procedures in place in the event of a key compromise? For example, key revocation lists.
- Is key revocation able to deal with simultaneity issues for multiple sites?
- Are customer system images protected or encrypted?

VII.3.4. Encryption

- Encryption can be used in multiple places − where is it used?
  - data in transit
  - data at rest
  - data in processor or memory?
- Usernames and passwords?
- Is there a well-defined policy for what should be encrypted and what should not be encrypted?
- Who holds the access keys?
- How are the keys protected?

VII.3.5. Authentication

- What forms of authentication are used for operations requiring high assurance? This may include login to management interfaces, key creation, access to multiple-user accounts, firewall configuration, remote access, etc.
- Is two-factor authentication used to manage critical components within the infrastructure, such as firewalls, etc?

VII.3.6. Credential compromise or theft

- Do you provide anomaly detection (the ability to spot unusual and potentially malicious IP traffic and user or support team behavior)? For example, analysis of failed and successful logins, unusual time of day, and multiple logins, etc
- What provisions exist in the event of the theft of a customer's credentials (detection, revocation, evidence for actions)?

VII.4. Asset management

It is important to ensure the provider maintains a current list of hardware and software (applications) assets under the cloud providers control. This enables checks that all systems have appropriate controls employed, and that systems cannot be used as a backdoor into the infrastructure.

- Does the provider have an automated means to inventory all assets, which facilitates their appropriate management?
- Is there a list of assets that the customer has used over a specific period of time?

The following questions are to be used where the end customer is deploying data that would require additional protection (i.e. deemed as sensitive).

- Are assets classified in terms of sensitivity and criticality?
  - If so, does the provider employ appropriate segregation between systems with different classifications and for a single customer who has systems with different classifications?

VII.5. Data and services portability

This set of questions should be considered in order to understand the risks related to vendor lock-in.

- Are there documented procedures and APIs for exporting data from the cloud?

- Does the vendor provide interoperable export formats for all data stored within the cloud?
- Are there processes for testing that data can be exported to another cloud provider – should the client wish to change provider, for example?
- Can the client perform their own data extraction to verify that the format is universal and is capable of being migrated to another cloud provider?

VII.6. Business continuity management

Providing continuity is important to an organization. Although it is possible to set service level agreements detailing the minimum amount of time systems are available, there remain a number of additional considerations.

- Does the provider maintain a documented method that details the impact of a disruption?
  - What are the RPO (recovery point objective) and RTO (recovery time objective) for services? Detail according to the criticality of the service.
  - Are information security activities appropriately addressed in the restoration process?
  - What are the lines of communication to end customers in the event of a disruption?
  - Are the roles and responsibilities of teams clearly identified when dealing with a disruption?
- Has the provider categorized the priority for recovery, and what would be our relative priority (the end customer) to be restored? Note: this may be a category (HIGH/MED/LOW).
- In the event of the primary site being made unavailable, what is the minimum separation for the location of the secondary site?

VII.7. Incident management and response

Incident management and response is a part of business continuity management. The goal of this process is to contain the impact of unexpected and potentially disrupting events to an acceptable level for an organization.

To evaluate the capacity of an organization to minimize the probability of occurrence or reduce the negative impact of an information security incident, the following questions should be asked to a cloud provider:

- Does the provider have a formal process in place for detecting, identifying, analyzing and responding to incidents?
- Is this process rehearsed to check that incident handling processes are effective? Does the provider also ensure, during the rehearsal, that everyone within the cloud provider's support organization is aware of the processes and of their roles during incident handling (both during the incident and post analysis)?
- How is the detection capabilities structured?
  - How can the cloud customer report anomalies and security events to the provider?
  - What facilities does the provider allow for customer-selected third party RTSM services to intervene in their systems (where appropriate) or to co-ordinate incident response capabilities with the cloud provider?
  - Is there a real time security monitoring (RTSM) service in place? Is the service outsourced? What kind of parameters and services are monitored?

- Do you provide (upon request) a periodical report on security incidents?
- For how long are the security logs retained? Are those logs securely stored? Who has access to the logs?

- How are severity levels defined?
- How are incidents documented and evidence collected?
- Besides authentication, accounting and audit, what other controls are in place to prevent (or minimize the impact of) malicious activities by insiders?
- Does the provider offer the customer (upon request) a forensic image of the virtual machine?
- How often does the provider test disaster recovery and business continuity plans?
- Does the provider collect data on the levels of satisfaction with SLAs?
- Does the provider carry out help desk tests? For example:
  - Impersonation tests (is the person at the end of the phone requesting a password reset, really who they say they are?) or so called 'social engineering' attacks.
- Does the provider carry out penetration testing? How often?
- Does the provider carry out vulnerability testing? How often?

VII.8. Physical security

As with personnel security, many of the potential issues arise because the IT infrastructure is under the control of a third party – like traditional outsourcing, the effect of a physical security breach can have an impact on multiple customers (organizations).

- What assurance can you provide to the customer regarding the physical security of the location?
  - Who, other than authorized IT personnel, has unescorted (physical) access to IT infrastructure? For example, cleaners, managers, 'physical security' staff, contractors, consultants, vendors, etc.
  - How often are access rights reviewed and how quickly can access rights be revoked?
  - Do you assess security risks and evaluate perimeters on a regular basis? How frequently?
  - Do you carry out regular risk assessments which include things such as neighboring buildings?
  - Do you control or monitor personnel (including third parties) who access secure areas?
  - What policies or procedures do you have for loading, unloading and installing equipment?
  - Are deliveries inspected for risks before installation?
  - Do network cables run through public access areas?
  - Do your personnel use portable equipment (e.g.,. laptops, smart phones) which can give access to the data centre? How are these protected?
  - What measures are in place to control access cards?
  - What processes or procedures are in place to destroy old media or systems when required to do so?
    - data overwritten?
    - physical destruction?

- What authorization processes are in place for the movement of equipment from one site to another?
    - How do you identify staff (or contractors) who are authorized to do this?

VII.9. Environmental controls

- What procedures or policies are in place to ensure that environmental issues do not cause an interruption to service?
- What methods do you use to prevent damage from a fire, flood, earthquake, etc?
- Do you monitor the temperature and humidity in the data centre?
- Do you protect your buildings from lightening strikes, including electrical and communication lines?
- Do you have stand-alone generators in the event of a power failure?
- Are all utilities (electricity, water, etc) capable of supporting your environment?
- Do you only allow authorized maintenance or repair staff onto the site?
- When equipment is sent away for repair, is the data cleaned from it first?

VIII.10. Legal requirements

Customers and potential customers of cloud provider services should have regard to their respective national and supra-national obligations for compliance with regulatory frameworks and ensure that any such obligations are appropriately complied with.

The key legal questions the customer should ask the cloud provider are:

- In what country is the cloud provider located?
- Is the cloud provider's infrastructure located in the same country or in different countries?
- Will the cloud provider use other companies whose infrastructure is located outside that of the cloud provider?
- Where will the data be physically located?
- Will jurisdiction over the contract terms and over the data be divided?
- Will any of the cloud provider's services be subcontracted out?
- Will any of the cloud provider's services be outsourced?
- How will the data provided by the customer and the customer's customers, be collected, processed and transferred?
- What happens to the data sent to the cloud provider upon termination of the contract?

CONCLUSIONS

The key conclusion is that the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective.

GLOSSARY AND ABBREVIATIONS

AAA	Authentication, authorization and accounting
AD	Active directory
API	Application programming interface - specification of interface published by software supplier
ARP	Address resolution protocol (2)
Asset	The target of protection in a security analysis
Availability	The proportion of time for which a system can perform its function
BS	British Standard
CA	Certification authority
CC	Common Criteria
Confidentiality	Ensuring that information is accessible only to those authorized to have access (ISO 17799)
Co-residence	Sharing of hardware or software resources by cloud customers
CP	Cloud provider
CRL	Certificate revocation list
CRM	Customer relationship management
Data controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.
Data processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Data subject	Identified or identifiable natural person (see EU Directive 95/46/EC) from whom data is collected and/or about whom that data is processed
DDoS	Distributed denial of service
De-provision	The process of enforcing the removal of a resource from use, or disallowing its use by a set of users
Edge network	In this context, a network of computers which is able to process and store data for delivery close to the final destination
EDoS	Economic denial of service
Escrow	The storage of a resource by a third party which has access to that resource when certain well-defined conditions are satisfied
FIM	Federated identity management
Guest OS	An OS under the control of the cloud customer, running in a virtualised environment
Host OS	The operating system of the cloud provider which runs multiple guest OSs
HSM	Hardware security module
Https	Http connection using TLS or SSL
Hypervisor	Computer software or hardware platform virtualization software that allows multiple operating systems to run on a host

	computer concurrently
IDS	Intrusion detection system
Integrity	The property that data has not been maliciously or accidentally altered during storage or transmission
IP	Internet protocol
IPS	Intrusion protection system
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MAC	Media access control (address of a network node in IP protocol)
MITM	Man in the middle (a form of attack)
MSS	Managed security services
NIS	Network and information security
NIST	National Institute of Standards and Technology (US)
Non-repudiation	The property whereby a party in a dispute cannot repudiate or refute the validity of a statement or contract
OCSP	Online Certificate Status Protocol
OS	Operating system
OTP	One-time password (type of authentication token)
OVF	Open virtualization format
Perimeterisation	The control of access to an asset or group of assets
Port scan	Probing a network host to determine which ports are open and what services they offer
Protection profile	A document specifying security evaluation criteria to substantiate vendors' claims of a given family of information system products (a term used in Common Criteria)
Provision	The issuing of a resource
PV LAN	Private VLAN
QoS	Quality of service
RBAC	Role-based access control
Resilience	The ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused)
ROI	Return on investment
ROSI	Return on security investment
RPO	Recovery point objective
RTO	Recovery time objective
RTSM	Real-time security monitoring
Security target	A document specifying security evaluation criteria to substantiate the vendor's claims for the product's security properties (a term used in Common Criteria)
Service engine	The system responsible for delivering cloud services
Side channel attack	Any attack based on information gained from the physical implementation of a system; e.g., timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system.
SLA	Service level agreement
SSL	Secure Sockets Layer (used for encrypting traffic between web servers and browsers)
Subpoena	In this context, a legal authority to confiscate evidence
TLS	Transport Layer Security (used for encrypting traffic between

	web servers and browsers)
ToU	Terms of use
UPS	Uninterruptable power supply
VLAN	Virtual local area network
VM	Virtual machine
VPC	Virtual private cloud
VPN	Virtual private network
Vulnerability	Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service
XML	Extensible Mark-up Language

REFERENCES

1. Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.
2. Gartner Says Worldwide IT Spending On Pace to Surpass Trillion in 2008, Gartner, 2008-08-18. Retrieved 2009-09-11.
3. "e-FISCAL project state of the art repository". http://www.efiscal.eu/state-of-the-art
4. "Jeff Bezos' Risky Bet", *Business Week*, http://www.businessweek.com/magazine/content/06_46/b4009001.htm
5. www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing

FCAPS, ITIL and TMN - Three key Ingredients of Architectural and Framework Standards in Network Management

LTC Gheorghe BARBU

CONTENTS

FCAPS, ITIL, and TMN - Three key Ingredients of Architectural and Framework Standards in Network Management

1. INTRODUCTION

Network management is a large and complex topic. In nowadays diverse networking infrastructure, the network concept has to handle more instances of unified communications, video, and virtualization.

As a generally rule, network management describes the methodology used to manage and maintain network operations and respond to user requirement changes. With the implementation of Simple Network Management Protocol (SNMP), the network (LAN or WAN) components can be monitored and managed, often from what is called a central Network Operations Center (NOC). The network management platform is an integrated suite of functions that can be implemented on one machine, or it can be implemented on several machines or databases spanning thousands of miles, supporting several organizations.

Network management can be segmented into two categories:

- Tactical — Tactical network management relates to proactive and reactive situations, such as network failures, congestion, and unacceptable service quality. The tasks include troubleshooting, configuration, and adjusting traffic flows.
- Strategic — Strategic network management involves a long-term perspective that is oriented toward adequate planning to avoid shortages as the network grows. Strategic tasks use information to adjust operations, optimize quality, and manage facilities to reduce overall operational costs.

So, the role of the network management process includes not only monitoring for performance and security, but also anticipating and estimating future network problems and transcending technology to ensure everything runs well together, whether it's the network, the server, or the application.

Network management means different things to different people. As example, for the Chief Information Officer of an organization it would mean being able to ensure that the enterprise IT infrastructure (consisting of departments, locations and services) is performing optimally. On the other side, from the point of view of the network administrator, network management is defined as a set of activities where a variety of tools, applications, rules and devices are utilized by IT personnel to monitor

and maintain information technology networks. To the network manager it would mean managing the details that constitute this high-level view.

2. ISSUES

In order to make an analysis with a more accuracy of what network management means, we need to find answers at the next questions:

2.1. What are the needs to be monitored?

First, we need to define the scope of the needs to be monitored and managed when we are dealing with networked applications.

Secondly, in order to provide satisfactory performance levels, we must be able to identify an array of problems that can have their source in the applications themselves, in the servers on which the applications run, or in the network. In the network, all resources (devices, applications, connections and configuration) can have an impact on the end-user service experience.

Finally, we have to determine how to resolve these problems. So, for assessing monitoring and management needs at a minimum level, we must plan to monitor:

2.1.1. End-user experience

We need to know whether there are response time problems before end users call the help desk or service desk to complain. We need to know whether a business application or service could fail or slow dramatically, threatening business revenues or institution image.

2.1.2. Servers, devices and applications in the network

We need to know if everything is configured correctly. Are servers performing correctly? Do performance level trends indicate an emerging problem? Is anything near a saturation point?

2.1.3. Traffic through the network

We need to identify which applications are consuming the most resources. Is the routing appropriate? Are there bottlenecks and when and why these could appear? Are some resources (hardware or software) over- or underutilized?

3. Which monitoring tools do we have on the market?

Once we understand what we need to monitor, we can move to inventory and assess which tools and application resources we have available to do that task today. Then, to determine what data and information is currently collected. This information

can provide insight into what is happening in the operational environment and how it will affect business service delivery and performance commitments. Knowing which tools and data we already have available that will allow determining the additional resources that we need in order to perform the overall management task.

4. Solutions

Nevertheless, we still have not achieved the expected results and in addition there are three frameworks which can use for understanding and taming network management: FCAPS, ITIL and TMN.

4.1. **FCAPS (F**ault-, **C**onfiguration-, **A**ccounting-, **P**erformance-, and **S**ecurity-) management, also called ISO Telecommunications Management Network, part of the OSI Network Management model, is an acronym for a categorical model of the working objectives of network management.

This model helps the network and system administrators to understand the major functions of network management systems and to provide knowledge to understand and surpass different issues in order to protect its environment. Without it, many system downtimes would occur and the organization may suffer a large financial or/and image loss.

This framework includes five levels:

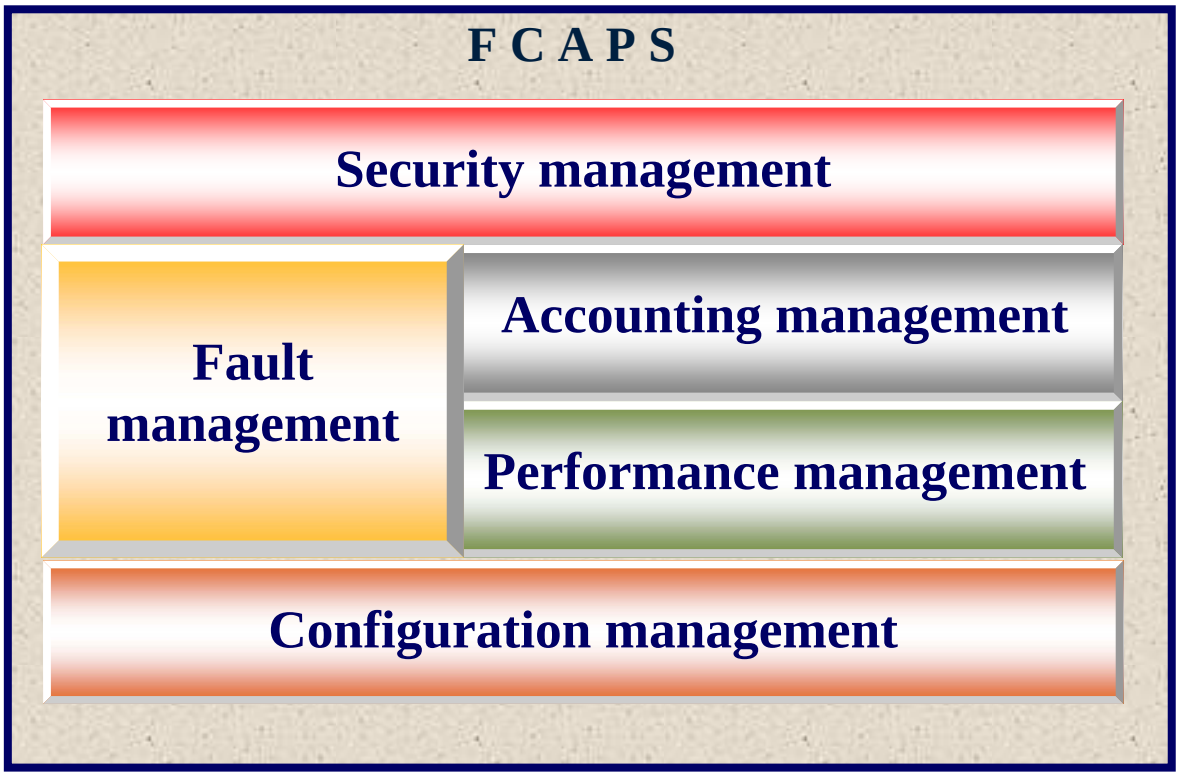


Fig. 1 FCAPS model levels

4.1.1. Level F—Fault management

At the F level, network problems are found and corrected. Potential future problems are identified, and steps are taken to prevent them from occurring or recurring. In this way, the network is kept operational, and downtime is minimized.

At this level, the aim is to recognize, isolate, correct, and log faults on the network. It is a system and network administrator duty to put in right place efficient monitoring tools to be alerted when faults exist. For example, you want to be alerted when something (e.g. a critical service) goes down on the network. If there is a fault, you have to test, fix, update, and repair any faults that occur on the network.

A common fault management technique is to implement an SNMP-based network management system (such as HP Open View) - to collect information about network devices.

4.1.2. Level C - Configuration management

At this level, network operations are monitored and controlled. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems, and removal of obsolete systems and programs, are coordinated. An inventory of equipment and programs is kept and updated regularly.

While it is possible to track these changes manually, a more common approach is to gather this information using configuration management software (such as Cisco Works 2000).

4.1.3. Level A - Accounting (allocation) management

The A level is for distributing resources optimally and fairly among network subscribers. This makes the most effective use of the systems available, minimizing the cost of operation. This level is also responsible for ensuring that users are billed appropriately.

Accounting Management is concerned with aspects of the system users. It mainly focuses on charging and billing users for services, and regulating service use (printing services, Internet/bandwidth, disk space usage, application and software use, etc.).

While this may not be applicable to all companies, in many larger organizations the IT department is considered a cost center that accrues revenues according to resource utilization by individual departments or business units.

4.1.4. Level P - Performance Management

The P level is involved with managing the overall performance of the network in order to meet the users and organizations desires. Performance management is

focused on ensuring that network performance remains at acceptable levels (the network and systems services must be available, the speed must be efficient, their must not be bottlenecks and the network should never be used to its maximum capacity for prolonged period of times and potential problems are identified). System and network administrators must actively monitor the network performance to ensure problems do not occur.

A major part of the effort is to identify which improvements will bring the greatest overall performance enhancement.

But Performance Management involves network analyze too in order to gather information so that you can prepare it for the future (because performance criteria of a network varies all the time).

4.1.5. Level S—Security Management

At the S level, the network is protected against hackers, unauthorized users, and physical or electronic sabotage. Confidentiality of user information is maintained where necessary or warranted. The security systems (controls overall activities and ensure data security through authentication and encryption) also allow network administrators to control what each individual authorized user can (and cannot) do with the system.

As a network and system administrator, we have to implement network authentication and security auditing tools to detect and prevent network sabotage, abuse and unauthorized access thereby:

- Record logs, Firewall setup
- Control spam, prevent viruses, Trojans, Spyware
- Upgrade software, install OS patches, implement authorization techniques and password.

4.2. ITIL - Information Technology Infrastructure Library

While the FCAPS framework is a great model for defining the objectives of network management, another best practices approach for service delivery was designed to align itself with current IT organizational structures and expand upon the FCAPS model. ITIL - ISO/IEC[1] 20000 (previously BS15000) is a standard developed in 2005 with a set of practices for IT service management that focuses on aligning IT services with the needs of business.

ITIL describes procedures, tasks and checklists (that are not organization-specific) used by an organization for establishing a minimum level of competency. It

[1] International Organization for Standardization and the International Electrotechnical Commission

allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

ITIL procedures are widely implemented in a lot of organizations all over the world (such as NASA, the UK National Health Service, etc). ITIL is also supported by quality services from a wide range of providers including examination institutes, accredited training providers and consultancies, software and tool vendors and well known service providers (IBM, HP and British Telecom, etc.).

ITIL is not a theoretical set of information and process descriptions. ITIL tries to adapt working processes in IT Infrastructure and the aims are:

- to reduce costs
- to provide high quality IT services
- to create a basis for quality management
- to have satisfied customers
- to have a better communication between customers and IT staff

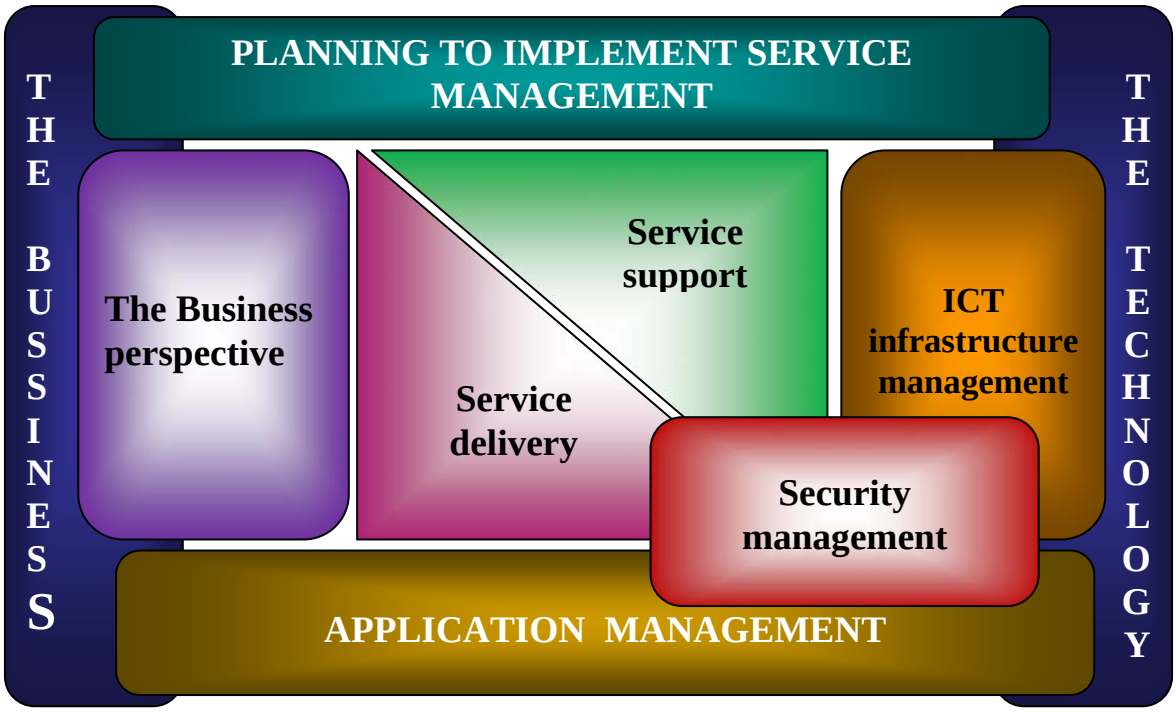


Fig. 2 – ITIL framework levels

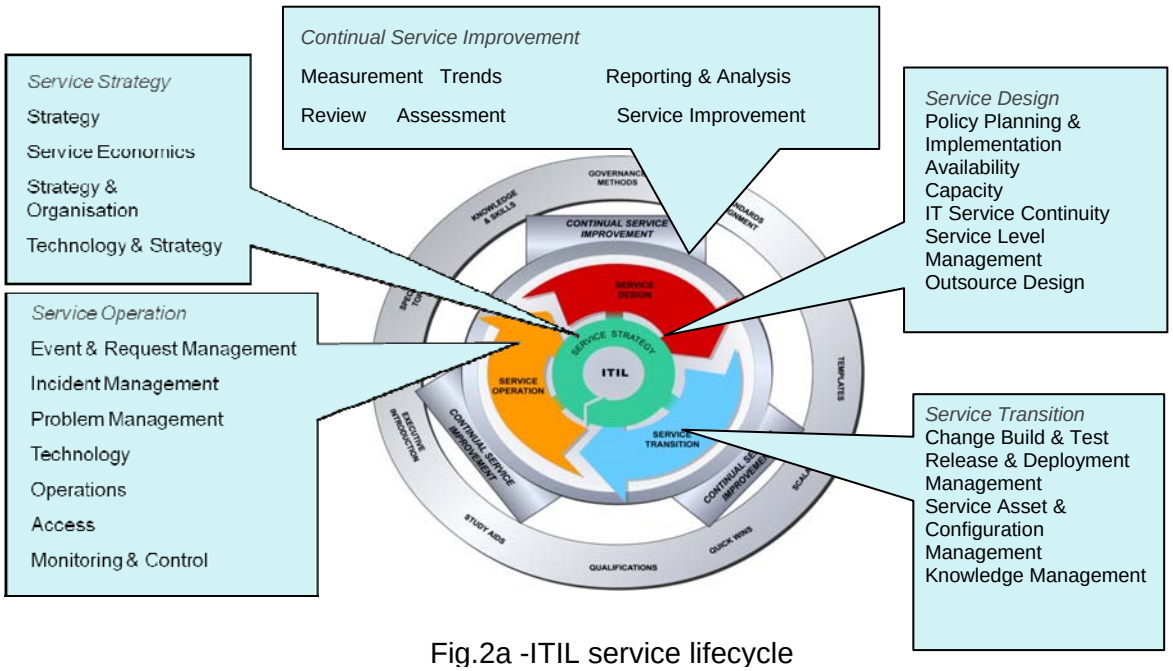


Fig.2a -ITIL service lifecycle

ITIL was designed to provide a better framework to deliver high-quality, consistent application delivery over a network infrastructure.

To reach the above described aims, the ITIL framework is defined by the next levels:

4.2.1. Business Management

According to the 2011 edition of ITIL, business service management (BSM) is "*the management of business services delivered to business customers. Business service management is performed by business units*."

Business Management can be used to understand the impact of business needs on IT services and infrastructure, helping in the process of planning to ensure the portfolio of Business Services and IT Services aim to support these changing needs and objectives. This approach also helps to understand how technology, including incidents, changes and new developments, impact the business and customers.

4.2.2. Application Management

Application management is designed with the sole purpose of ensuring that an application has the right configuration and design to be implemented in the network environment. This discipline can cover many various aspects of network management, from number of application dependencies to delay timers for satellite links. Application management is designed to ensure that the application, end-to-end, is fully enabled to provide the service and delivery to the end users.

4.2.3. Service delivery

For many organizations, this is typically for network operations centre (NOC). The service delivery process begins by defining the services to be delivered, the target consumers of the service, the business requirements and motivators for the services, and other high-level business issues.

The service delivery level is focused to ensuring to the end users the applications that they require. This area focuses on aspects of troubleshooting, help desk, and supporting new applications over the network. Problems management would track the number of incidents and facilitate troubleshooting of faults or performance problems that occur in the environment.

To troubleshoot a network environment, a good understanding of what devices are on the network and their configuration is handled by the configuration management (often called as configuration management database - CMDB). Change management also involves both aspects of problem management and configuration management as the change board would approve planned changes for the infrastructure, update the CMDB, and record any problems encountered during the change.

4.2.4. Service Support

IT Service Management (ITSM) is concerned with delivering and supporting IT services that are appropriate to the business requirements of the organization. ITIL is fast becoming an international de facto standard, providing a complete, consistent and coherent set of best practices for IT Service Management, promoting a quality approach for achieving business effectiveness and efficiency in the use of information systems. Service Support focuses on ensuring that the customer has access to appropriate services to support business functions. Issues covered include Service Desk, Incident Management, Problem Management, Configuration Management, Change Management and Release Management.

4.2.5. Security Management

A basic concept of security management is the information security and the primary goal of information security is to guarantee safety of information (the confidentiality, integrity and availability). The goal of the Security Management is split up in two parts:

- The realization of the security requirements defined in the service level agreement (SLA) and other external requirements which are specified in underpinning contracts, legislation and possible internal or external imposed policies;

- The realization of a basic level of security. This is necessary to guarantee the continuity of the management organization. This is also necessary in order to reach a simplified service-level management for the information security, as it happens to be easier to manage a limited number of SLAs than it is to manage a large number of SLAs.

Security Management involves protecting a network from all kinds of unauthorized access. This includes many sub functions like collecting and reporting security related information, proactively detecting and preventing intrusions, etc.

Security Management covers the following aspects:

- Intrusion Detection for Network and Host–(E.g. OSSEC, Prelude Hybrid IDS, Snort, Suricata, Nessus, etc.)
- Configuration Management of remote nodes (E.g. Mercurial, Rancid)
- Analysis of data collected at the remote nodes (E.g. Nagios, Sysmon)
- Taking action based on analyzed data
- Real-time response to certain types of intrusions

4.2.6. Information and Communication Technology (ITC) Infrastructure Management

In larger organizations, the teams that design and troubleshoot the systems are separate entities than the team that installs the equipments. This is why an accurate configuration management is essential to the success of IT organizations. Infrastructure management is responsible for the installation and physical configuration of all network devices in the organization. When changes are approved by the configuration management team, infrastructure teams are the army that enforces these changes based on the designs by other architects and engineers.

Software asset management is often considered a vital aspect of managing an organization. Software licenses and products are expensive commodities. Software asset management is designed to be partially configuration management as it provides essential information about the software installed on each device, its revision or platform level, and how many instances are required. Accounting for proper licensing and software maintenance is a big business with many larger IT organizations.

4.3. Telecommunications Management Network (TMN) Framework

TMN standardization started in 1985 by CCITT[2] Study Group as an infrastructure to support management and deployment of telecommunications services. It provides a framework for achieving interconnectivity and communications across various operating systems and telecommunications networks. Most popular aspect of TMN is the suggested layer model. These are described in figure no. 3.

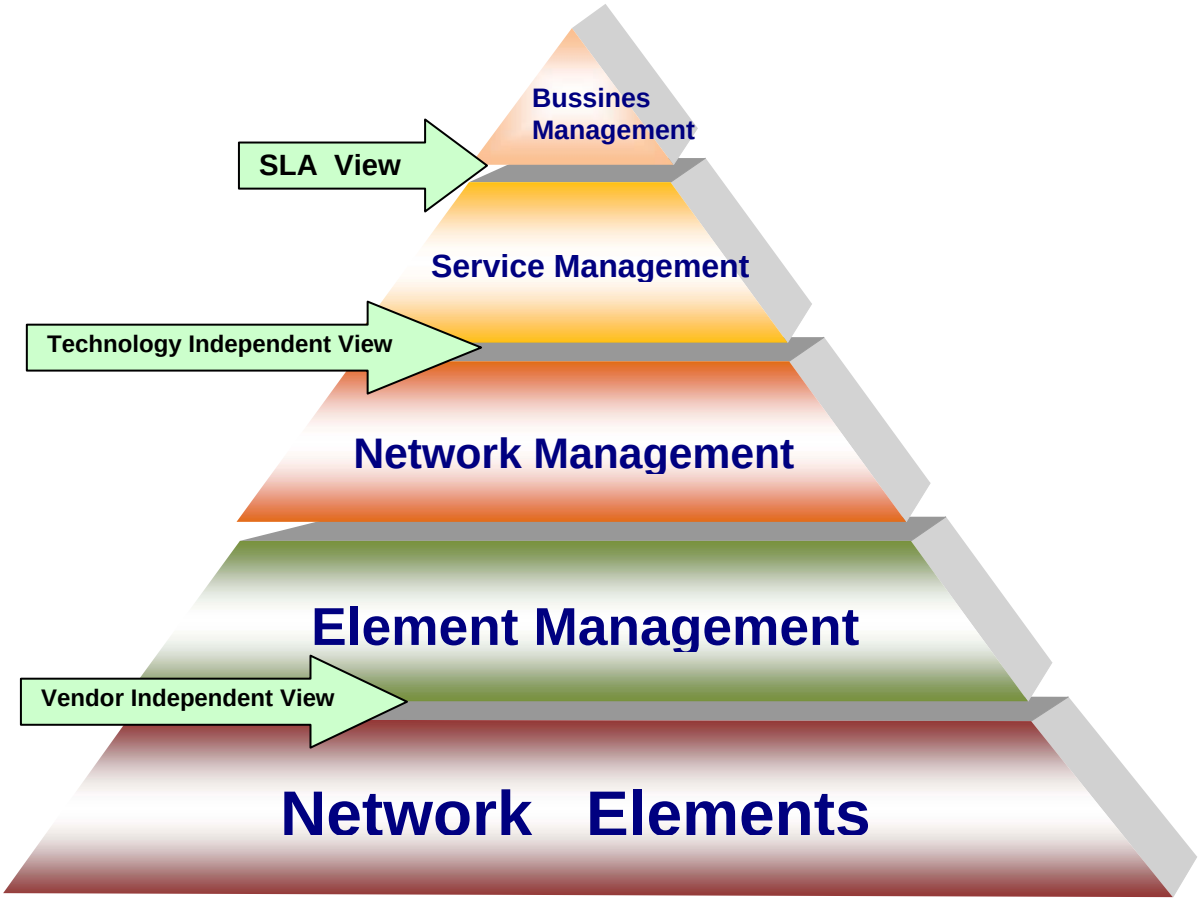


Fig. 3 - TMN pyramid

The layers identified in TMN framework are:

- Network Elements Layer
- Network Management Layer
- Service Management Layer
- Business Management Layer

4.3.1. Networks Elements Layer

A typical telecommunication network consists of exchanges and transmission systems. In TMN terminology, exchanges and transmission systems are examples of network elements. Network Elements layer defines interfaces for the network

[2] Comité Consultatif International Téléphonique et Télégraphique

elements, instantiating functions for device instrumentation, ideally covering all FCAPS areas.

4.3.2. Element Management Layer

Applications in this layer are referred as Element Management System (EMS) or Element Manager in short. An EMS has direct connectivity with Network Elements and it provides remote access to most of the NE controls, to EMS operator. Using an EMS, an operator can monitor and control the network element at maximum granularity. Typically, each equipment vendor provides its respective EMS to manage its network elements. There is separate EMS for each technology. For example, if a service provider uses network elements provided by Huawei as well as Ericsson for a GSM network, then there will be one EMS provided by Huawei to manage its elements and a separate EMS provided by Ericsson to manage its respective elements. In another example, if a service provider provides both 2G and 3G services, then usually, it will have separate EMSs for both the technologies, to manage their respective network elements.

4.3.3. Network Management Layer

Applications in this layer are referred to as Network Management System (NMS). NMS is a manager of managers. An NMS does not have direct connectivity with Network Elements, rather it is connected with multiple EMSs. NMS manages the network over a layer of abstraction. Typically, an NMS has multi-vendor and multi-technology support. That means an NMS manages EMSs from multiple vendors and there might be a single NMS to manage both 2G as well as 3G networks. Since NMS are not tightly coupled with network elements, therefore usually they are provided by third-party vendors.

HP OpenView, TeMIP, SMARTS, IBM Netcool are popular third-party NMS products.

4.3.4. Service Management Layer

Applications in this layer are often referred as service assurance application, service activation & fulfillment application and service trouble management application. These applications work on another layer of abstraction.

First step for design of service management layer is service modeling, where all services offered by a service provider are identified along with resources that power those services. This information is captured in a service graph. Service assurance applications are designed to determine the impact of problems in resources, on each service offered by the service provider. Examples of these

services are voice and data service, MMS, caller tunes in case of GSM. Since each service provider has unique set of service offerings, therefore often a service management solution is tailor-made for each service provider, utilizing available generic products and frameworks.

4.3.5. Business Management Layer

Applications in this layer are meant for decision support. For example a service provider will like to know which of the service offered is under-utilized and which one is over-utilized, so that decision can be taken regarding allocation of future-funds. Similarly there are applications to design service products and track their lifecycle. And Customer Relationship Management also comes under this layer.

5. Conclusions

A simply review of these standards shows that ITIL, TMN, and FCAPS overlap in terms of concept that they address. It is true that they do speak some of the same concept (for example, see figure no. 4) but they do so at completely different levels of abstraction.

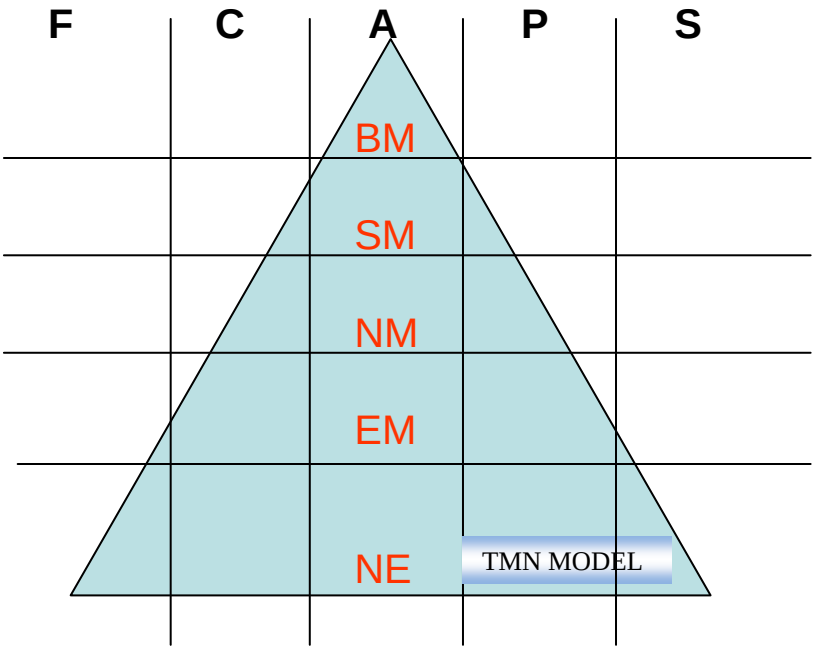


Fig. 4 – Grid relations between FCAPS and TMN frameworks

Summing up:

There is no clear answer regarding which is better, FCAPS, or TMN. Each one of these is a framework of best practices, not a prescriptive manual.

- FCAPS is similar to the OSI[3] Reference Model, primarily focused on the concept of **technology management**. Starting with a technology centric view, FCAPS is the methodology used to implement the TMN standards for network management. FCAPS is a major contributor to network management used to implement the network management architecture
- TMN is based on the OSI management framework and it focuses on **service management** (TMN presents technology at a level that the business can understand; not just by the network administrator). Providing a unified interface to all network elements, networks and services to be managed, the TMN model helps to categorize, prioritize, and specify the responsibilities of telecommunications management products and services. TMN will continue as a framework for telecommunications management.
- ITIL is all about the process for how to run an efficient IT organization (ITIL focuses on **process and workflow**).

On the other side, FCAPS has proven to be a logical and low risk starting point. As a recommendation for IT leadership (these levels of sophistication are direct addressed to them), start with FCAPS concepts and put a plan in place to optimize the organization by developing ITIL best practices based on TMN concepts.

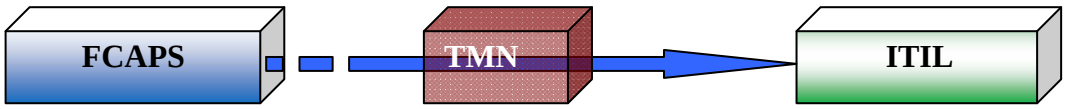


Fig. 5 A good approach for adoption of IT management (suggestion).

By understanding and implementing TMN, FCAPS or ITIL concepts in order to build adequate infrastructures, companies can maximize the value of their current systems and equipment and be ready for the future.

[3] **Open Systems Interconnection model** (ISO/IEC 7498-1)

6. REFERENCES

[1] Neil Greenfield -*FCAPS Management for the Smart Grid High-level Summary* , May 6, 2009

[2] Shirley Lacy, Frieda Midgley, Nigel Williamson -*ITIL® Managing Digital Information Assets*, White Paper January 2011

[3] Valerie Arraj, White Paper- *ITIL: The Basics*, May 2010

[4] Jim Clinch White - *ITIL V3 and Information Security*, Paper, May 2009

[5] Christos Gkantsidis and Hitesh Ballani - *Network Management as a Service*

[6] Rob England- *Review of recent ITIL® studies For APMG,* White Paper, November 2011

[7] Theophilus Benson - *Unraveling the Complexity of Network Management*

[8] Jeff Parker - *FCAPS, TMN and ITIL –Three key ingredients to effective IT management*, May 6, 2005

[9] Michael Faber and Rubina Faber - *ITIL and Corporate Risk Alignment Guide. An introduction to corporate risk and ITIL, and how ITIL supports and is assisted by Management of Risk*, March 2010

[10] Sandra Whittleston - *ITIL® is ITIL* , University of Northampton, March 2012

[11] *Everything you wanted to know about ITIL® in less than one thousand words!*- White Paper, October 2007

[12] Alison Cartlidge and others- *An Introductory Overview of ITIL® V3*, 2007

[13] http://www.iec.orgWeb - *Proforum Tutorials*

[14] http://wiki.hsc.com/wiki/Main/ Telecommunications Management Network - *Web Proforum Tutorials*

[15] http://en.wikipedia.org/wiki/Wikipedia- *Proforum Tutorials*

F-16 FIGHTING FALCON MULTIROLE FIGHTER - ROMANIAN CHOISE FOR REBUILDING AIR FORCE ARHITECTURE

CAPT.CDOR Cătălin COLŢĂNEL

CONTENTS

F-16 FIGHTING FALCON MULTIROLE FIGHTER - ROMANIAN CHOISE FOR REBUILDING AIR FORCE ARHITECTURE

INTRODUCTION

Once Romania join to NATO in 2004, some commitments had to be achieved by the Air Forces, on short, medium and long terms. National Defense Staff vision at that time included renew of fight aircraft flota starting with 2009-2010.

But economic and social crises raised in this time, forced the Staff to change vision and postpone year after year decision taking. Changing vision consist of decreasing number of aircraft aimed to be purchased (from 48 to 24, then to 12) , postpone milestones and deadline of project. Nevertheless, in the latest years, Romania has forced to find a solution for replacing Mig-21 Lancer whit another multirole airplane. In my opinion, decision seems to be taken: used F-16 Falcon (most probable Block 25) is appropriate to be purchased by Romanian Air Forces.

The F-16 Falcon was designed by General Dynamics from early 1970s but is now a product of Lockheed-Martin. This plane was designed to have good performance in climbing and turning flight. The F-16 first flew in 1974, and more than 4000 have been built The first of the US Air Force multi-role fighter aircraft, is the world's most prolific fighter with more than 2,000 in service with the SUAVE and 2,000 operational with 25 other countries.[1]

. The F-16 and the F-15 Eagle were the world's first aircraft able to withstand higher g-forces than the pilots. The Fighting Falcon entered service in 1979. The last of 2,231 F-16 fighters for the US Air Force was delivered in March 2005. The first two-seat F-16D version was accepted by the US Government in January 2009.

Foreign orders have included Bahrain (ten delivered), Greece (60 block 52 all delivered), Israel (50), Egypt (24 block 40), New Zealand (28), United Arab Emirates (80 block 60, first delivered 2005), Singapore (20), South Korea (20 block 52 all delivered), Oman (12), Chile (ten block 50) and Poland (48 block 52).

[1] http://www.aero-web.org/events/perform/tb/f16.htm

I. MISSION OF THE F-16 FIGHTING FALCON

F-16 multi-mission fighters flew a variety of missions which include suppression of enemy air defense, offensive counter air, defensive counter air, air interdiction, close air support and forward air controller missions. Mission results were outstanding as these fighters destroyed radar sites, vehicles, tanks, enemy's aircrafts and buildings.

Whether F-16 Fighting Falcon is a compact, multi-role fighter aircraft, is highly maneuverable and has proven itself in air-to-air combat and air-to-surface attack. It provides a relatively low-cost, high-performance weapon system for any air force allover the world.

Its electronic equipment and most advanced IT features make this airplane able to perform a large number of different missions, both of air to ground and air to air, as highest accuracy as possible at this time. The conflicts which in were involved proved its versatility and effectiveness, even we speak about conflicts during cold war or the 21st century conflicts.

II. F-16 FALCON EQUIPMENTS AND FEATURES

II.1. F-16 Fighting Falcon cockpit

Advanced equipment being fitted on the current build of the F-16 includes Honeywell color flat-panel liquid crystal multifunction displays, digital terrain system, modular mission computer, color video camera to record the pilot's view of the head-up display (HUD), a color triple-deck video recorder and an enhanced programmable display generator.

Under the USAF project Sure Strike, the F-16 is equipped with an improved data modem (IDM), which automatically provides target data to the HUD using data transmitted by a ground observer.

The seat-back angle of the aircraft has been increased from 13° to 30° to provide increased comfort for the pilot.

Follow-on programmed, project Gold Strike, integrates an upgraded IDM for the transmission of images to and from a range of sources, including ground units and unmanned aircraft. The system can transmit images from the LANTIRN targeting pod and display video imagery to the cockpit.

USAF F-16 aircraft receive the Boeing joint helmet-mounted cueing system (JHMCS), currently in full-rate production. Deliveries of production systems began in 2004 and the system was first deployed operationally during Operation Iraqi Freedom.

II.2. F-16 missiles and weapons

USAF F-16 aircraft receive the Boeing joint helmet-mounted cueing system (JHMCS), currently in full-rate production. Deliveries of production systems began in 2004, the system was first deployed operationally during Operation Iraqi Freedom.
The aircraft has nine hard points for weapons payloads: one at each wing tip, three under each wing and one centerline under the fuselage. The ordnance is launched from Raytheon LAU-88 launchers, MAU-12 and bomb ejector racks. The port wing is fitted with a 20mm General Electric M61A1 multi-barrel cannon and the gun sight is interfaced to the cockpit HUD.

Air-to-air missiles which have been carried on the F-16 include the Lockheed Martin / Raytheon AIM-9 Sidewinder, Raytheon AMRAAM, Raytheon Sparrow, MBDA (formerly Matra BAe Dynamics) Skyflash and ASRAAM, and the MBDA R550 Magic 2. In April 2004, the F-16 first fired the new-generation AIM-9X Sidewinder, which is in full-rate production for the USAF.

Air-to-surface missiles carried on the F-16 include Maverick, HARM and Shrike missiles, manufactured by Raytheon, and anti-ship missiles include Boeing Harpoon and Kongsberg Penguin. Flight tests with the Lockheed Martin joint air-to-surface stand-off missile (JASSM) have been conducted from the F-16.

The first guided launch of the new joint direct attack munitions (JDAM) was successfully carried out from an F-16. The F-16 was the first USAF aircraft to be fitted with the joint stand-off weapon (JSOW) in April 2000.

The F-16 can be fitted with Lockheed Martin wind-corrected munitions dispenser (WCMD), which provides precision guidance for CBU-87, -89, and 97 cluster munitions. The system corrects for launch transients, ballistic errors, and winds aloft. [2]

The F-16 will be the first aircraft to use the USAF's new weapon rack, the Edo Corporation BRU-57. The BRU-57 is a vertical ejection rack which doubles the aircraft's capacity for precision-guided weapons like JDAM and WCMD.

[2] http://www.janes.ea.com/janes/awa/f16.htm

All-weather stand-off weapons such as the AGM-84E stand-off land-attack missile (SLAM) and the AGM-142 Popeye II are planned to be included in future upgrades to the aircraft. Other advanced weapons include MICA, IRIS-T, Python IV, Active Skyflash air-to-air missile, ALARM antiradiation missile, Apache multimission stand-off weapon, autonomous free-flight dispenser system and AS30L laser-guided missile.

II.3. Targeting

The aircraft has nine hard points for weapons payloads: one at each wing tip, three under each wing and one centerline under the fuselage. The ordnance is launched from Raytheon LAU-88 launchers, MAU-12 and Orgen bomb ejector racks. The port wing is fitted with a 20mm General Electric M61A1 multi-barrel cannon and the gunsight is interfaced to the cockpit HUD.

Air-to-air missiles which have been carried on the F-16 include the Lockheed Martin / Raytheon AIM-9 Sidewinder, Raytheon AMRAAM, Raytheon Sparrow, MBDA (formerly Matra BAe Dynamics) Skyflash and ASRAAM, and the MBDA R550 Magic 2. In April 2004, the F-16 first fired the new-generation AIM-9X Sidewinder, which is in full-rate production for the USAF.

Air-to-surface missiles carried on the F-16 include Maverick, HARM and Shrike missiles, manufactured by Raytheon, and anti-ship missiles include Boeing Harpoon and Kongsberg Penguin. Flight tests with the Lockheed Martin joint air-to-surface stand-off missile (JASSM) have been conducted from the F-16.

The first guided launch of the new joint direct attack munitions (JDAM) was successfully carried out from an F-16. The F-16 was the first USAF aircraft to be fitted with the joint stand-off weapon (JSOW) in April 2000.

The F-16 can be fitted with Lockheed Martin wind-corrected munitions dispenser (WCMD), which provides precision guidance for CBU-87, -89, and 97 cluster munitions. The system corrects for launch transients, ballistic errors, and winds aloft.

The F-16 will be the first aircraft to use the USAF’s new weapon rack, the Edo Corporation BRU-57. The BRU-57 is a vertical ejection rack which doubles the aircraft's capacity for precision-guided weapons like JDAM and WCMD.

All-weather stand-off weapons such as the AGM-84E stand-off land-attack missile (SLAM) and the AGM-142 Popeye II are planned to be included in future

upgrades to the aircraft. Other advanced weapons include MICA, IRIS-T, Python IV, Active Skyflash air-to-air missile, ALARM antiradiation missile, Apache multimission stand-off weapon, autonomous free-flight dispenser system and AS30L laser-guided missile.

The F-16 carries the Lockheed Martin LANTIRN infrared navigation and targeting system. This is used in conjunction with a BAE Systems holographic display. Block 50/52 aircraft are equipped with the HARM Targeting System, AN/ASQ-213 from Raytheon.

US Air National Guard F-16 aircraft are fitted with Northrop Grumman Litening II / Litening ER targeting pods.

In August 2001, Lockheed Martin was selected to provide the Sniper XR as the new advanced targeting pod for USAF F-16 and F-15E aircraft. Sniper XR (extended range) incorporates a high-resolution mid-wave FLIR, dual-mode laser, CCD TV, laser spot tracker and laser marker combined with advanced image processing algorithms. Deliveries began in March 2003.

F-16 fighters for Oman were been equipped with BAE Systems advanced airborne reconnaissance system. Those for Poland and Morocco were been equipped with the Goodrich DB-110 reconnaissance pod.

II.4 Radar

The Northrop Grumman AN/APG-68 radar provides 25 separate air-to-air and air-to-ground modes, including long-range, all-aspect detection and tracking, simultaneous multiple-target tracking, and high-resolution ground mapping. The planar antenna array is installed in the nose of the aircraft.

An upgraded version of the radar, AN/APG-68(V) 9, has begun flight testing. The upgrade features: 30% increases in detection range five times increase in processing speed, ten times increase in memory, as well as significant improvements in all modes, jam resistance and false alarm rate.

II.5 Navigation and communications

The F-16 was the first operational US aircraft to receive a global positioning system (GPS). The aircraft has an inertial navigation system, either a Northrop Grumman (Litton) LN-39, LN-93 ring laser gyroscope or Honeywell H-423.

"The F-16 Fighting Falcon carries the Lockheed Martin LANTIRN infrared navigation and targeting system."

Other navigation equipment includes a BAE Systems Terprom digital terrain navigation system, Gould AN/APN-232 radar altimeter, Rockwell Collins AN/ARN-118 tactical air navigation system (TACAN) and Rockwell Collins AN/ARN-108 instrument landing system.

The communications systems include the Raytheon UHF AN/ARC-164 receiver / transmitter and Rockwell Collins VHF AM/FM AN/ARC-186 together with AN/APX101 identification friend or foe (IFF) and encryption / secure communications systems. The AN/APX-101 is being upgraded with BAE Systems AN/APX-113.

II.6 Engines

The aircraft is powered by a single engine: the General Electric F110-GE-129 or Pratt and Whitney F100-PW-229. The fuel supply is equipped with an inert gas anti-fire system. An in-flight refueling probe is installed in the top of the fuselage.

Lockheed Martin has completed developmental flight testing on new conformal fuel tanks (CFT) for the F-16, which will significantly add to the aircraft's mission radius. First flight of the F-16 equipped with the new tanks was in March 2003. Greece is the launch customer for the CFT.

II.7 Countermeasures

Block 50 F-16 aircraft for the USA are equipped with the Lockheed Martin super heterodyne AN/ALR-56M radar warning receiver. The F-16 is also compatible with a range of jammers and electronic countermeasures equipment, including Northrop Grumman AN/ALQ-131, Raytheon AN/ALQ-184, Elisra SPS 3000 and Elta EL/L-8240, and the Northrop Grumman ALQ-165 self-protection suite.

Lockheed Martin ALE-40 and ALE-47 chaff and infrared flare dispenser systems are installed in an internal flush mount. ALE-40 is pilot-controlled but the ALE-47 installed in block 50 can be operated in fully, semi-automatic or manual mode. [3]

F-16s for the Greek Air Force are being fitted with the Raytheon advanced self-protection integrated suite (ASPIS) II which includes Northrop Grumman ALR-93(V) threat warning system, Raytheon ALQ-187 jammer and BAE Systems ALE-47 chaff / flare dispenser.

[3] http://www.dfrc.nasa.gov/EAO/FactSheets/F_16XLFACTS.html

F-16s for Chile and Pakistan are fitted with the ITT AN/ALQ-211 (V) 4 electronic warfare suite.

III. F-16 FIGHTING FALCON INTERNATIONAL ORDERS AND DELIVERIES

The F-16 Fighting Falcon is the world's most prolific fighter.

Israel, with the world's largest F-16 fleet outside the USAF, has ordered 110 F-16I aircraft, of which the first was delivered in December 2003. These aircraft have Pratt & Whitney F100-PW-229 engines, Elbit avionics, Elisra electronic warfare systems and Rafael weapons and sensors, including Litening II laser target designator pods. Italy has leased 34 aircraft until the first tranche of Eurofighter deliveries are completed. Hungary will acquire 24 ex-USAF fighters. [4]

In December 2005, Greece ordered a further 30 block 52+ fighters (20 F-16C single seat and 10 F-16D two-seat) to be delivered from 2009. Under the Peace Xenia IV purchase programme, the total number of fighters ordered by Greece's HAF (Hellenic Air Force) rose to 170. The first Peace Xenia IV F-16 block 52 advanced aircraft was delivered on 19 March 2009. The remaining was delivered by 2010.

In June 2005, Pakistan requested the foreign military sale (FMS) of 36 F-16C/D block 50/52 aircraft. In June 2006, the Pentagon notified congress of its intention to agree the sale and Lockheed Martin was awarded a contract for 12 F-16C and six F-16D block 52 aircraft in December 2006. The aircraft are armed with AMRAAM and Sidewinder missiles and the Sniper targeting pod. The planned order of the second 18 aircraft was cancelled.

In September 2006, Turkey requested the sale of an additional 30 advanced block 50 F-16 aircraft. The order was signed in May 2007. The aircraft were delivered in 2011 and 2012. The total cost of these additional aircraft is estimated at more than $2.9bn excluding Turkey's $1.1bn upgrade programme for its existing F-16 fleet.

In December 2007, Morocco requested the sale of 24 F-16C/D block 50/52 aircraft. The deal includes the aircraft, mission equipment and a support package provided by Lockheed Martin and other US and international contractors. The Royal Moroccan Air Force (RMAF) placed a $233.6m order in June 2008.

The F-16IN Super Viper, which is a development of block 60, has been designed for the Indian Air force. It is a fourth-generation fighter that meets the

[4] http://www.lmtas.com/FighterPrograms/F16/index.html

medium multirole combat aircraft (MMRCA) requirements. It includes Northrop Grumman APG-80 AESA radar and General Electric F110-132A engine with 32,000lb thrust.

Various F-16 upgrade and modernization programmers are underway in Turkey, Pakistan and Jordan, and within the US Air Force. Future upgrades include air refueling probes, auxiliary power unit, auto ground collision avoidance systems and automatic maneuvering attack.[5]

IV. F-16 COMMON CONFIGURATION IMPLEMENTATION PROGRAMME (CCIP)

650 USAF blocks 40/50 F-16s are being upgraded under the common configuration implementation programme (CCIP).

The first phase of the programme (first aircraft completed in January 2002) provides core computer and color cockpit modifications.

The second, who began in September 2002, involves fitting the advanced AN/APX-113 interrogator / transponder and Lockheed Martin Sniper XR advanced FLIR targeting pod.

The third, which started in July 2003, adds Link 16 data link, the Boeing joint helmet-mounted cueing system and an electronic horizontal situation indicator. Operational testing of the M3 upgraded fighters was completed in September 2004. Deliveries were completed in 2010.

A 216 block 40/50 F-16 aircraft of the Turkish Air Force are to be upgraded with elements of the CCIP, under an agreement reached in April 2005. Lockheed Martin was awarded the contract to supply the modernization kits in December 2006. The upgrade is scheduled for completion in 2016.

The export version of the Sniper XR pod, the PANTERA, has been ordered by the Royal Norwegian Air Force. The first was delivered in November 2003.

Block 50/52 is the eighth major modification block of the F-16 that incorporates color cockpit displays, new electronic warfare suite, advanced weapons and sensors and more powerful engine.

[5] http://www.f-16.net/reference.html

CONCLUSIONS

F-16 Falcon is a great weapon and fit Romanian Air Forces with it is the best thing can be done. In my opinion, there are at least three reasons take into consideration performing this action:

- affordability (thinking about drop defense budget);
- easy conversion for pilots (MIGs avionics is almost the same);
- open way for further transition to the F-35 Joint Strike Fighter.

But it is important for Romania to proceed in this attempt without mistakes as well. Some issues have to be solved in the best manner: pilot conversion and training, building airport infrastructure, maintenances and logistic aspects are only couple of them.

REFERENCES

1. http://www.aero-web.org/events/perform/tb/f16.htm
2. http://www.janes.ea.com/janes/awa/f16.htm
3. http://www.dfrc.nasa.gov/EAO/FactSheets/F_16XLFACTS.html
4. http://www.lmtas.com/FighterPrograms/F16/index.html
5. http://www.f-16.net/reference.html

CURRENT ISSUES IN NETWORK SECURITY MANAGEMENT

LTC Doru SĂPUNARU

CONTENTS

CURRENT ISSUES IN
NETWORK SECURITY MANAGEMENT

OVERVIEW

One of the primary goals of computer and network security is the protection of company assets. By "assets," I do not mean the hardware and software that constitute the company's computers and networks. The assets are comprised of the "information" that is housed on a company's computers and networks. Information is a vital organizational asset. Network and computer security is concerned, above all else, with the protection, integrity, and availability of information. Information can be defined as data that is organized and accessible in a coherent and meaningful manner. Security measures and countermeasures are implanted to protect organizations from different security attacks. To guarantee the security requirements of a given organization, it is essential to be able to evaluate the current security demands of an organization as well as the measures taken to achieve such requirements. Security weaknesses cause a negative impact on organizations such as financial loss, reputations, and loss of customer confidence.

The intention of implementing security measures, controls, and policies is to guard information security objectives and information assets. Information security objectives, which are confidentiality, integrity, and availability, are the main concern in categorizing information security level. It is important to remember that information security is not just about protecting assets from outside hackers. The majority of the time threats are internal to an organization: "We have found the enemy and it is us."

I. NETWORK SECURITY

I.1. Introduction

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security

involves the authorization of access to data in a network, which is controlled by the network administrator. Network security covers a variety of computer networks, both public and private. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done.

Network security management is by nature a distributed function. Applications that may utilize security management include firewalls, databases, Email, teleconferencing, electronic commerce, intrusion detection, and access control applications. Security management faces the same security threats as other distributed applications. Coordinated management of security is not feasible without a secure management infrastructure that protects in transit messages from modification, spoofing, and replay. Although end system security is beyond the scope of this discussion, it is clear that key management, access control, and reliable implementation of management software are critical also.

It is also important to remember that network security is not absolute. All security is relative. Network security should be thought of as a spectrum that runs from very unsecure to very secure. The level of security for a system or network is dependent on where it lands along that spectrum relative to other systems. It is either more secure or less secure than other systems relative to that point. There is no such thing as an absolutely secure network or system.

Network security involves protecting all the resources on a network from threats. You must consider not only the computers on the network, but other network devices, network transmission media, and the data being transmitted across the network.

Network security is a balancing act that requires the deployment of "proportionate defenses." The defenses that are deployed or implemented should be proportionate to the threat. Organizations determine what is appropriate in several ways, described as follows:

• Balancing the cost of security against the value of the assets they are protecting;

• Balancing the probable against the possible;

• Balancing business needs against security needs.

I.2. The Security Trinity

The three legs of the "security trinity," prevention, detection, and response, comprise the basis for network security. The security trinity should be the foundation for all security policies and measures that an organization develops and deploys.

I.2.1 Prevention

The foundation of the security trinity is prevention. To provide some level of security, it is necessary to implement measures to prevent the exploitation of vulnerabilities. In developing network security schemes, organizations should emphasize preventative measures over detection and response: It is easier, more efficient, and much more cost-effective to prevent a security breach than to detect or respond to one. Remember that it is impossible to devise a security scheme that will prevent all vulnerabilities from being exploited, but companies should ensure that their preventative measures are strong enough to discourage potential criminals-so they go to an easier target.

I.2.2 Detection

Once preventative measures are implemented, procedures need to be put in place to detect potential problems or security breaches, in the event preventative measures fail. It is very important that problems be detected immediately. The sooner a problem is detected the easier it is to correct and cleanup.

I.2.3 Response

Organizations need to develop a plan that identifies the appropriate response to a security breach. The plan should be in writing and should identify who is responsible for what actions and the varying responses and levels of escalation.

Before beginning a meaningful discussion on computer and network security, we need to define what it entails. First, network security is not a technical problem; it is a business and people problem. The technology is the easy part. The difficult part is developing a security plan that fits the organization's business operation and getting people to comply with the plan.

Next, companies need to answer some fundamental questions, including the following.

• How do you define network security?

• How do you determine what is an adequate level of security?

To answer these questions, it is necessary to determine what you are trying to protect.

I.3. Security models

There are three basic approaches used to develop a network security model. Usually, organizations employ some combination of the three approaches to achieve security. The three approaches are security by obscurity, the perimeter defense model, and the **defense in depth model.**

I.3.1 Security by Obscurity

Security by obscurity relies on stealth for protection. The concept behind this model is that if no one knows that a network or system is there, then it won't be subject to attack. The basic hope is that hiding a network or at least not advertising its existence will serve as sufficient security. The problem with this approach is that it never works in the long term, and once detected, a network is completely vulnerable.

I.3.2 Perimeter Defense

The perimeter defense model is analogous to a castle surrounded by a moat. When using this model in network security, organizations harden or strengthen perimeter systems and border routers, or an organization might "hide" its network behind a firewall that separates the protected network from an untrusted network. Not much is done to secure the other systems on the network. The assumption is that perimeter defenses are sufficient to stop any intruders so that the internal systems will be secure.

There are several flaws in this concept: First, this model does nothing to protect internal systems from an inside attack. As we have discussed, the majority of attacks on company networks are launched from someone internal to the organization. Second, the perimeter defense almost always fails eventually. Once it does, the internal systems are left wide open to attack.

I.3.3 Defense in Depth

The most robust approach to use is the defense in depth model. The defense in depth approach strives for security by hardening and monitoring each system;

each system is an island that defends itself. Extra measures are still taken on the perimeter systems, but the security of the internal network does not rest solely on the perimeter systems. This approach is more difficult to achieve and requires that all systems and network administrators do their part. With this model, however, the internal network is much less likely to be compromised if a system administrator on the network makes a mistake like putting an unsecured modem on the system. With the defense in depth approach, the system with the modem may be compromised, but other systems on the network will be able to defend themselves. The other systems on the network should also be able to detect any attempted hacks from the compromised system. This approach also provides much more protection against an internal intruder. The activities of the internal intruder are much more likely to be detected.

II. SOLUTION - DEFENSE IN DEPTH

II.1. Introduction

Defense in depth is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. The principle of defense-in-depth is that layered security mechanisms increase security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system. For example, it is not a good idea to totally rely on a firewall to provide security for an internal-use-only application, as firewalls can usually be circumvented by a determined attacker (even if it requires a physical attack or a social engineering attack of some sort). Other security mechanisms should be added to complement the protection that a firewall affords (e.g., surveillance cameras, and security awareness training) that address different attack vectors.

Defense in depth minimizes the probability that the efforts of malicious hackers will succeed. A well-designed strategy of this kind can also help system administrators and security personnel identify people who attempt to compromise a computer, server, proprietary network or ISP (Internet service provider). If a hacker gains access to a system, defense in depth minimizes the adverse impact and gives

administrators and engineers time to deploy new or updated countermeasures to prevent recurrence.

Components of defense in depth include antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection and biometric verification. In addition to electronic countermeasures, physical protection of business sites along with comprehensive and ongoing personnel training enhances the security of vital data against compromise, theft or destruction.

While no solution exists for perfect security in today's complex environment, Defense in Depth is the methodology that provides the greatest balance between protection and risk tolerance through a multilayered approach to address a broad array of exposure.

A complete Defense in Depth approach will include most or all of the following tools:

- Packet filtering firewall with state full packet inspection
- DMZ for isolated, externally-facing servers
- Application layer firewall with deep packet inspection
- Intrusion detection/prevention
- Proxy server
- Wireless network authentication and encryption
- Antivirus protection for network, file servers and clients
- Spam filtering at server and client
- Content monitoring and filtering
- Mobile device validation
- Host-Based firewall for servers and clients
- Patch management
- Access control policies based on the principal of least privilege
- Strong password policy
- Workstation lockdown rules
- Application security features
- Appropriate use of data encryption
- User policies and training

II.2. Adversaries, Motivations, Classes of Attack

To effectively resist attacks against its information and information systems, an organization needs to characterize its adversaries, their potential motivations, and

their classes of attack. Potential adversaries might include: Nation States, Terrorists, Criminal Elements, Hackers, or Corporate Competitors. Their motivations may include: intelligence gathering, theft of intellectual property, denial of service, embarrassment, or just pride in exploiting a notable target. Their classes of attack may include: passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through the industry providers of one's Information Technology resources.

It's also important to resist detrimental effects from non-malicious events such as fire, flood, power outages and user error.

II.3. Information Assurance

Information Assurance is achieved when information and information systems are protected against such attacks through the application of security services such as: Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. The application of these services should be based on the Protect, Detect, and React paradigm. This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks.

Fig.1 Principles of Defense in Depth strategy

An important principle of the Defense in Depth strategy is that achieving Information Assurance requires a balanced focus on three primary elements: People, Technology and Operations.

II.3.1 People

Achieving Information Assurance begins with a senior level management commitment (typically at the Chief Information Officer level) based on a clear understanding of the perceived threat. This must be followed through with effective Information Assurance policies and procedures assignment of roles and responsibilities, commitment of resources, training of critical personnel (e.g. users and system administrators), and personal accountability.

This includes the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of the Information Technology environment.

II.3.2 Technology

Today, a wide range of technologies are available for providing Information Assurance services and for detecting intrusions. To insure that the right technologies are procured and deployed, an organization should establish effective policy and processes for technology acquisition. These should include: security policy, Information Assurance principles, system level Information Assurance architectures and standards, criteria for needed Information Assurance products, acquisition of products that have been validated by a reputable third party, configuration guidance, and processes for assessing the risk of the integrated systems.

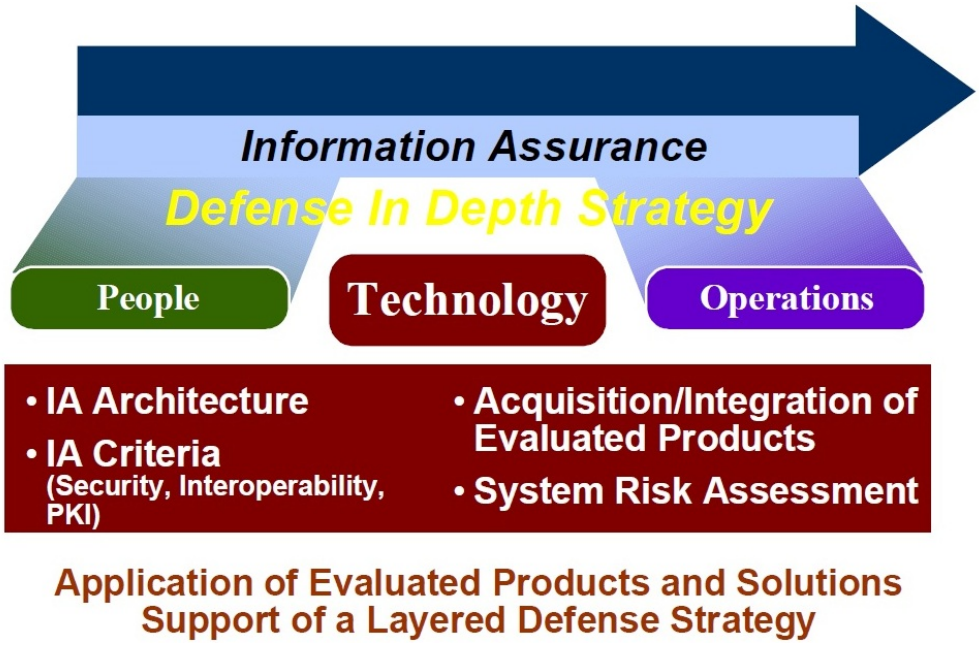


Fig.2 Elements of Technology

The Defense in Depth strategy recommends several Information Assurance principles. These include:

a) **Defense in Multiple Places**. Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to deploy protection mechanisms at multiple locations to resist all classes of attacks. As a minimum, these defensive "focus areas" should include:

Fig.3 Defense in Depth Focus Areas

• Defend the Networks and Infrastructure

-Protect the local and wide area communications networks (e.g. from Denial of Service Attacks)

-Provide confidentiality and integrity protection for data transmitted over these networks (e.g. use encryption and traffic flow security measures to resist passive monitoring)

• Defend the Enclave Boundaries (e.g. deploy Firewalls and Intrusion Detection to resist active network attacks)

• Defend the Computing Environment (e.g. provide access controls on hosts and servers to resist insider, close-in, and distribution attacks).

b) **Layered Defenses**. Even the best available Information Assurance products have inherent weaknesses. So, it is only a matter of time before an adversary will find an exploitable vulnerability.

An effective countermeasure is to deploy multiple defense mechanisms between the adversary and his target. Each of these mechanisms must present

unique obstacles to the adversary. Further, each should include both “protection” and “detection” measures.

Examples of Layered Defenses

Class of Attack	*First Line of Defense*	*Second Line of Defense*
Passive	Link & Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and Personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and Personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

Fig.4 Examples of Layered Defenses

These help to increase risk (of detection) for the adversary while reducing his chances of success or making successful penetrations unaffordable. Deploying nested Firewalls (each coupled with Intrusion Detection) at outer and inner network boundaries is an example of a layered defense. The inner Firewalls may support more granular access control and data filtering.

c) **Specify the security robustness** (strength and assurance) of each Information Assurance component as a function of the value of what’s it is protecting and the threat at the point of application. For example, it’s often more effective and operationally suitable to deploy stronger mechanisms at the network boundaries than at the user desktop.

d) **Deploy robust key management and public key infrastructures** that support all of the incorporated Information Assurance technologies and that are highly resistant to attack. This latter point recognizes that these infrastructures are lucrative targets.

e) **Deploy infrastructures to detect intrusions** and to analyze and correlate the results and react accordingly. These infrastructures should help the “Operations” staff to answer questions such as: Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options?

II.3.3 Operations

The operations leg focuses on all the activities required to sustain an organization's security posture on a day to day basis.

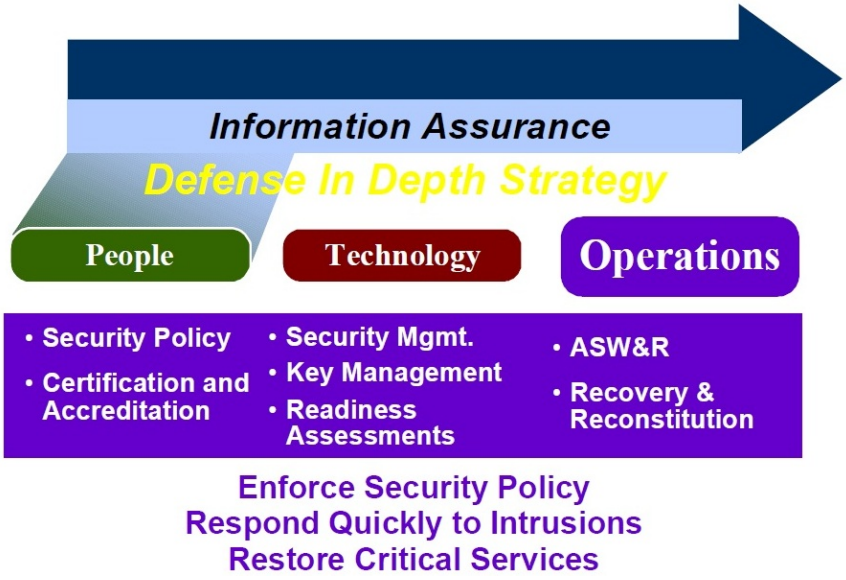


Fig.5 Elements of Operations

These include:

a) Maintaining visible and up to date system security policy

b) Certifying and accrediting changes to the Information Technology baseline. The C&A processes should provide the data to support "Risk Management" based decisions. These processes should also acknowledge that a "risk accepted by one is a risk shared by many" in an interconnected environment.

c) Managing the security posture of the Information Assurance technology (e.g. installing security patches and virus updates, maintaining access control lists)

d) Providing key management services and protecting this lucrative infrastructure

e) Performing system security assessments (e.g. vulnerability scanners, RED teams) to assess the continued "Security Readiness"

f) Monitoring and reacting to current threats

g) Attack sensing, warning, and response

h) Recovery and reconstitution

III. INFORMATION SYSTEMS SECURITY ASSESSMENT

III.1. Introduction

Risk is the possibility that some incident or attack will cause damage to an organization's network. An attack consists of a sequence of actions that attempts to exploit weak points in an organization's practices or its network configuration. To assess the risk posed by the attack you have to evaluate the amount of potential damage and the likelihood that the attack will occur. This likelihood will depend on the attacker's motivation and on how easy it is to mount the attack. In turn, this will further depend on the security configuration of the system under attack. The process of identifying a risk and assessing its likelihood and impact is known as risk analysis.

The concept of risk assessment is crucial to developing proportionate defenses. To perform a risk analysis, organizations need to understand possible threats and vulnerabilities. The first step in risk analysis is to identify assets, vulnerabilities, and threats, and to rank them according to their value (assets), impact on the business if they are exploited (vulnerabilities), and likelihood of occurrence (threats).The basic steps for risk assessment are listed as follows:

1. Identifying and prioritizing assets;
2. Identifying vulnerabilities;
3. Identifying threats and their probabilities;
4. Identifying countermeasures;
5. Developing a cost benefit analysis;
6. Developing security policies and procedures.

To identify and prioritize information assets and to develop a cost benefit analysis, it is
helpful to ask a few simple questions such as the following.

- What do you want to safeguard?
- Why do you want to safeguard it?
- What is its value?
- What are the threats?
- What are the risks?
- What are the consequences of its loss?
- What are the various scenarios?
- What will the loss of the information or system cost?

III.1.2. Assets

First, assets have to be identified and valued. In an IT system, assets include the following:

▲ Hardware: laptops, desktops, servers, routers, PDAs, mobile phones, smart cards, and so on.

▲ Software: applications, operating systems, database management systems, source code, object code, and so on.

▲ Data and information: essential data for running and planning your business, design documents, digital content, data about your customers, data belonging to your customers (like credit card numbers), and so forth.

▲ Reputation: the opinion held by your customers and the general public about your organization. Reputation can affect how likely a person is to place an order with you or provide you with information.

Many areas of engineering and business have developed their own disciplines and terminology for risk analysis. Within IT security, risk analysis is applied:

▲ Comprehensively for all information assets of an enterprise.

▲ Specifically for the IT infrastructure of an enterprise.

▲ During the development of new products or systems—for example, in the area of software security.

Today, the evaluation of Information Systems (IS) security in accordance with business requirements is a vital component of any organizations business strategy. While there are a few information security assessment standards, methodologies and frameworks that talk about what areas of security must be considered, they do not contain specifics on HOW and WHY existing security measures should be assessed, nor do they recommend controls to safeguard them.

The reason for which you have to run a vulnerability assessment is to check that all systems have been patched for vulnerability, or obtain a list of systems that require a patch. This is a great way to verify that your patch management software actually did its job and rolled out the patches.

Vulnerability assessments (VA) can be broken down into three steps: information gathering/discovery, enumeration, and detection.

III.2. Information Gathering/Discovery

Information gathering is used to determine the breath of the assessment by gathering IP addresses, available port information, and possible contact information of the target.

Information gathering and discovery is the process an individual or group performs to ascertain the breath/scope of an assessment. The purpose of this step is to identify and determine the total number of systems and applications that will be assessed. Output of this step typically consists of host names, Internet Protocol (IP) addresses, available port information, and possibly target contact information.

III.3. Enumeration

Enumeration validates the underlying operating system and running applications of the target.

Enumeration is the process used to determine the target operating system—a process called OS fingerprinting—and the applications that reside on it. Upon determining the operating system, the next step is to substantiate the applications that reside on the host.

III.4. Detection

Detection determines what vulnerabilities exist.

Detection is the method used to determine whether a system or application is susceptible to attack (i.e., vulnerable).This step doesn't confirm that vulnerabilities exist; penetration tests do that. The detection process only reports the likelihood that vulnerabilities are present.

To detect vulnerabilities we'll need to utilize a vulnerability assessment tool such as Tenable Network Security's Nessus or eEye Digital Security's Retina. Neither tool is free, so we'll need to evaluate the cost or pursue open source alternatives prior to conducting this step.

Once we have procured a VA tool, we can continue the assessment, targeting the systems we've evaluated in steps 1 and 2 to determine whether they have any vulnerabilities. VA tools detect vulnerabilities by probing remote systems and comparing the systems' response to a set of good (expected) and bad (vulnerable)

responses. If the VA tool receives what it considers a bad response it assumes the host is vulnerable.

III.5. Detecting Vulnerabilities via Security Technologies

Traditionally when we want to ascertain system- or application-level vulnerabilities, we need to install vulnerability assessment scanners throughout our enterprise.

These scanners are responsible for detecting network hosts (information gathering), discovering available applications (enumeration), and ascertaining vulnerabilities (detection). Vulnerability assessments scanners are typically network appliances running VA software. Figures 1 represent a typical organization's VA infrastructure.

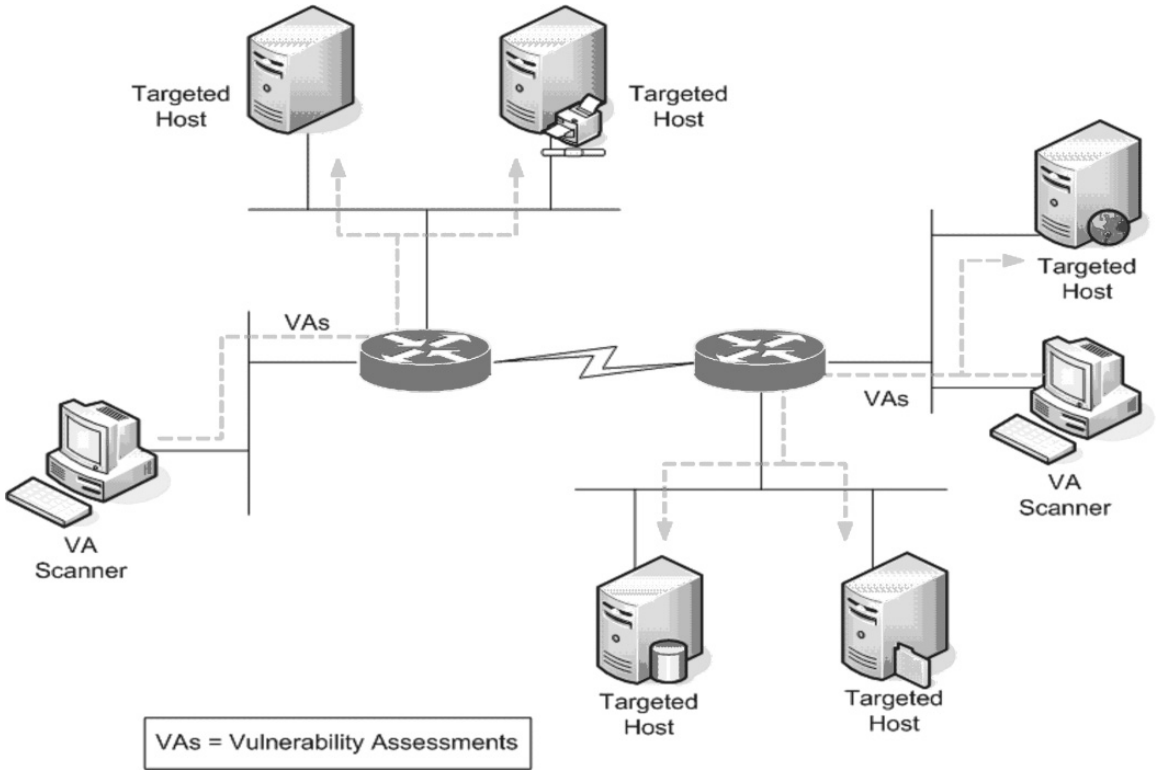


Fig.6. An enterprise VA deployment

IV. CONCLUSIONS

With the increased number of threats to networks such as worms, viruses and clever hackers, security can no longer be viewed as an option, even within “private” networks. Securing all equipment, including physical infrastructure equipment such as UPS systems and HVAC systems, is critical to maintaining uptime and seamless access to services. Providing and maintaining security across the enterprise typically means increased administration. Historically, this has been the largest barrier to broad implementations of security.

Today, the amount of time spent repairing a network due to just a single worm or virus attack can easily be greater than the upfront time to more adequately secure an enterprise. Fortunately, there are many options in systems and software to increase the security of the network while reducing the overhead of managing such systems. Even basic practices such as periodic software updates, locking down all devices and using centralized authentication and secure access methods can go a long way to reducing risks. Institution of appropriate security policies and frequent network audits further increase the overall protection of the network.

REFERENCES

1. John E. Canavan- *Fundamentals of Network Security*, 2001.
2. Christopher Leidigh -*Fundamental Principles of Network Security*, 2005.
3. Christopher J. May, Josh Hammerstein, Jeff Mattson -*Defense in Depht* , 2006.
4. J. Christopher Wells -*Defense in Depht*: *Strategies for Information Security*, 2007.
5. Steve Manzuik, Ken Pfeil, Andre Gold-*Network Security Assessment*, 2007.

CRITICAL INFRASTRUCTURE PROTECTION - A CHALLENGE FOR TODAY WORLD

LTC Florian STANCU

CONTENTS

CRITICAL INFRASTRUCTURE PROTECTION MANAGEMENT - A CHALLENGE FOR TODAY WORLD

INTRODUCTION

On January 1st 2007, Romania became a member of the European Union after the Treaty of Accession, signed on 25 April 2005, has been ratified by all Member States. Its geographic position put Romania in the border role of European Union and NATO. These facts involve more strategic challenges in order to secure Romanian territory and implicitly active participation in European Union and NATO security. That means more Romanian capabilities have to become part of a significant political, economic, social and military system.

Recent events occurring worldwide that focused action on national interest objectives that have influence on economic and social life, shows how vulnerable we are certain areas or sectors that provide essential services to all areas of social life.

In this context, more attention should be paid to these areas of interest that are directly aimed at civil society, and national security, in accordance with the magnitude and negative consequences that may result from disruption of the functioning of these areas or sectors.

I. DEFINING CRITICAL INFRASTRUCTURES

I.1. INFRASTRUCTURES

"The term infrastructure has been used since 1927 to refer collectively to the roads, bridges, rail lines, and similar public works that are required for an industrial economy, or a portion of it, to function. The term also has had specific application to the permanent military installations necessary for the defense of a country. Perhaps because of the word's technical sound, people now use infrastructure to refer to any substructure or underlying system. Big corporations are said to have their own financial infrastructure of smaller businesses, for example, and political organizations to have their infrastructure of groups, committees, and admirers."

The American Heritage Dictionary of the English Language, Fourth Edition

"Infrastructures can be considered all building and permanent installations necessary for the support, redeployment, and military forces operations (e.g.

barracks, headquarters, airfields, communications, facilities, stores, port installations, and maintenance stations)."

Dictionary of Military and Associated Terms. US Department of Defense 2005.

Infrastructures are part of a resistance structure system are relational and functional and is necessary support for the system to identify, individualize, to enter into relations with other systems to stabilize and obviously work. Depending on the place, role and importance for the stability and system functionality and safety and security systems and processes infrastructures can be divided into three main categories:

- Common infrastructure;
- Special infrastructure;
- Critical infrastructures.

Common infrastructure is a structure, a framework, providing construction and functioning of the system. This infrastructure does not have special qualities other than justifying of the existence and presence in systems and processes. Examples: roads, railways, municipalities, schools, libraries, etc. Along the time, some can become special or critical, depending on the new role its can have, dynamic of importance and other criteria.

Special infrastructures have an important role in the functioning of systems and processes, providing them hi efficiency, quality, comfort and performance. As a rule, special infrastructures are the performance infrastructures. Some of them, especially those which may have, by extension or by transformation (modernization), an important role in the stability and security of systems can ascend into the category of critical infrastructures.

I.2. CRITICAL INFRASTRUCTURES

To define critical infrastructures and to distinguish them from other infrastructures is a key challenge for policy-makers, and one that has been addressed in different ways by national governments.

There are several definitions of critical infrastructure in official policy documents and in the literature.

The European Commission defines critical infrastructures as:

"An asset, system or part thereof located in member states that are essential for the maintenance of vital societal functions, health, safety, security, economic or

social well-being of people, and the disruption or destruction of which would have a significant impact on a member state as a result of the failure to maintain those functions."

European Council Directive 2008/114/CE

The definition of critical infrastructures is now a moving target. Many countries around the world adopt different definition of critical infrastructures according with political, social, economic and cultural background of the area.

Let's see on the next several definitions of critical infrastructure from different countries, revealing important differences in the way the issue is addressed at the policy level.

"Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defense and ensure national security."

Australia: "What is critical infrastructure?" (www.ag.gov.au/agd)

"Canada's critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada."

Canada: "About Critical Infrastructure", Public Safety Canada (www.ps-sp.gc.ca)

"Critical infrastructures are organizations and facilities of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences."

Germany: "Critical Infrastructure Protection in Germany",
Federal Office for Information Security (www.bsi.de).

"The [Critical National Infrastructure] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: 1) cause large scale loss of life; 2) have a serious impact on the national economy; 3) have other grave social consequences for the community; or 3) be of immediate concern to the national government."

United Kingdom: "Protecting the Critical National Infrastructure"
(www.security.homeoffice.gov.uk).

The general definition of critical infrastructure in the overall US critical infrastructure plan is: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." For investment policy purposes, this definition is narrower: “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security."

United States: “National Infrastructure Protection Plan” (2006) (www.dhs.gov).

According to Romanian legislation on the Romanian territory critical infrastructures are, National Critical Infrastructures and European Critical Infrastructures.

National Critical Infrastructure (ICN) an element or a part of them, situated on national territory, that it is essential for the maintenance of vital functions of society, health, safety, security, economic or social well-being of people and whose disruption or destruction would have a nationally significant impact because of the failure to maintain those functions.

European Critical Infrastructure (ICE) a national critical infrastructure whose disruption or destruction would have a significant impact on at least two member states of the European Union.

II. CRITICAL INFRASTRUCTURES PROTECTION (CIP)

Critical Infrastructure Protection (CIP) includes any activity that aims to ensure the functionality and integrity of critical infrastructures to deter, mitigate and neutralize a threat, risk or vulnerability.

The European Union face more challenges in critical infrastructure protection policy. In the past few years, the European Commission has adopted a number of policy initiatives in this field, including Directives and Communications to promote the enhancement of preparedness, security and resilience. However, a number of outstanding problems remain because member states are at varying degrees of maturity with respect to the development of a comprehensive and effective CIP policy.

To achieve an effective system of critical infrastructure protection the key are to identify critical systems and infrastructures, inventory and audit existing capabilities, identify interdependencies and major actions and milestones and develop a strong system of policy and clear understanding of mandate.

II.1. IDENTIFYNG CRITICAL INFRASTRUCTURES

After terrorist attacks of 11 September 2001 on the complex World Trade Center and the Pentagon, it is considered that an infrastructure is or may become a critical infrastructure in relation to terrorist attacks or other threats, particularly asymmetric. This is only one aspect or criterion for identifying infrastructure critical. However, there are others that take both, so stability and functionality of systems and processes and their relations with the external environment. Therefore, analysis of critical infrastructure issues must take into account all dimensions and implications of stability and functionality systems and processes, and causal chain that can generate or influence their dynamics.

At national level are established criteria for identifying critical infrastructure such as:

- Victims criterion, evaluated according to the number of possible deaths and injuries;
- Criterion of economic, evaluated according to the importance of economic loss and degradation of products or services, including any environmental impacts
- Effect on the population criterion evaluated according to its impact on the trust, physical suffering and disruption of daily life, including loss of essential services.

The infrastructure that will meet all the criteria including those set forth in the definition of critical infrastructure will be selected as critical infrastructure at governmental level.

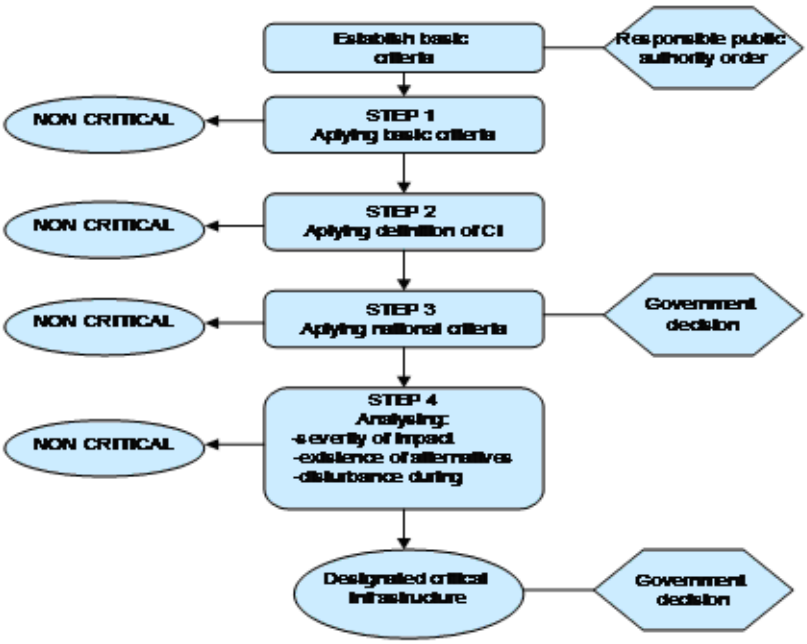


Figure 1. The process of identifying and selecting critical infrastructure

The table below presents the main sectors and sub-sectors of critical infrastructure:

Table 1. Critical infrastructures and key resources

Sector	Sub-sector
Energy	Oil and gas production, refining, treatment, storage and distribution by pipelines Electricity generation and transmission
Nuclear industry	Production and storage/processing of nuclear substances
Information, Communication Technologies, ICT	Information system and network protection Instrumentation automation and control systems (SCADA etc.) Internet Provision of fixed telecommunications Provision of mobile telecommunications Radio communication and navigation Satellite communication Broadcasting
Water	Provision of drinking water Control of water quality Stemming and control of water quantity
Food	Provision of food and safeguarding food safety and security
Health	Medical and hospital care Medicines, serums, vaccines and pharmaceuticals Bio-laboratories and bio-agents
Financial	Payment and securities clearing and settlement infrastructures and systems Regulated markets

Sector	Sub-sector
Transport	Road transport Rail transport Air transport Inland waterways transport Ocean and short-sea shipping
Chemical industry	Production and storage/processing of chemical substances Pipelines of dangerous goods (chemical substances)
Space	Space
Research facilities	Research facilities

II.2. INTERDEPENDENCIES

Progressively, our lives have become dependent on a number of pieces of infrastructure, such as roads, the electricity grid, the networked environment, financial services and the internet. We perform many activities and satisfy many of our primary needs thanks to these types of infrastructure. Relying on critical infrastructure allows us to act more economically and efficiently. This also means, however, that the disruption of infrastructure may damage our economies substantially and lead to natural disasters and loss of human life.

Several governments and organizations around the world have concluded that critical infrastructures are increasingly vulnerable and interdependent with other critical infrastructures. The relevance of some infrastructures for the continuity of government, for business operations and for the supply of basic services to citizens has become so high that a disruption of any of these fundamental assets can cause considerable damage.

A real challenge of protecting critical infrastructures is a well understanding of the interdependencies between them and applies this principle in a strong system of policy.

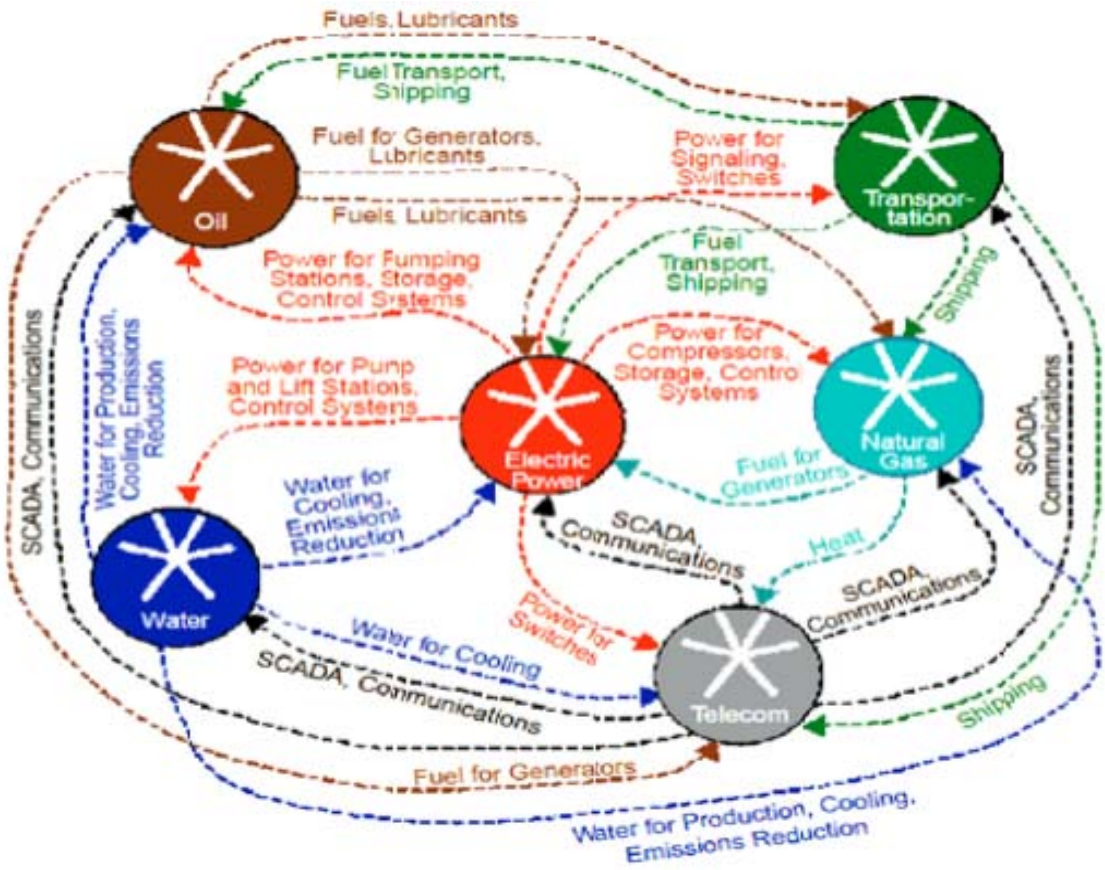


Figure 2. Example of interdependencies.

Kenneth Neil Cukier (The economist 2005) offer an interesting reading of what happened on September 11, 2001 witch offer an example of interdependencies and resilience:

"After the second plane crashed into the South Tower at 9:02 am, telephone calls increased up to ten times the normal traffic volume – so much congestion that only a handful could get through. Major news Web sites – CNN, the BBC, The New York Times and others – were so clogged with traffic they became temporarily unreachable. By 9:39 am many radio stations in the city went dark (most broadcasters had transmitters on the towers). When the first tower collapsed at 10:05 am, and then the second at 10:28 am, they destroyed a vast amount of telecom infrastructure in the vicinity, complicating communications even more.

To be sure, in many instances the systems proved resilient. For instance, network technicians struggling to repair systems coordinated their activities using mobile text messages since their cell phones couldn't handle calls. And as many noted afterwards, the internet worked when the phone system didn't. Indeed, at 9.54

pm the Federal Emergency Management Agency alerted all stations to prepare in case primary communications methods failed – and did this, ironically, by email.

But here is the nub: as bad as all this sounds, the actual event did not do too much damage to the information infrastructure – yet subsequent problems with other networks began to cause havoc. For instance, a fire at a building on the periphery of the World Trade Center knocked out a power station upon which telecoms equipment elsewhere depended. A falling beam from an unstable building in the vicinity crashed into an operator's central switching office, damaging the machines. By late evening, systems that had survived went down simply because they overheated. And telecom services were disrupted when backup generators ran out of fuel because trucks carrying new provisions were blocked from entering lower Manhattan.

In short, the incident highlights both the vulnerability and resilience of information infrastructure – and importantly, its interdependence with other infrastructures. For instance, the communications network is dependent on the electrical grid; the back-up generators are dependent on the roadway network. And of course, it bears noting, that the target of the attack in New York was not communications infrastructure at all, but two office buildings. What might have been the consequences if critical information infrastructure had been targeted as well?"

II.3. THE PUBLIC-PRIVATE PARTNERSHIP

Because at the present most important capabilities are owned by the private sector and the state is the main responsible actor in the protection of critical infrastructure is strongly required a public-private partnership to ensure protection of critical infrastructure. The main milestones of the definition of framework of cooperation could be:

- Critical infrastructure protection is a shared responsibility of the state sector and private;

- Government must provide adequate environment (in terms of legal, managerial and technological) for private firms to invest in critical infrastructure elements;

- The solution of relationship "State-private sector" in critical infrastructure protection can be a mixed system comprising a minimal set of standardized regulations and appoint an independent third partner to control and evaluate partnership activities.

In the European Union, the European Commission set up a European Program for Critical Infrastructure Protection (EPCIP) that incorporates all analyzes and criteria measures. The program is designed to identify critical infrastructure, analyze vulnerabilities, dependencies and interdependencies and find solutions to their security.

The program objectives are:

- Identification and inventory by governments of states member, of critical infrastructures located on the territory of each State, in accordance with the priorities established by EPCIP.

- The collaboration between owner companies and governments to disseminate information and reduce the risk of incidents which could cause extensive or durable disturbance of critical infrastructure;

- The common approach to security of critical infrastructure, thanks to all public and private collaboration.

European program intends, among others, to join in a network, all experts in critical infrastructure protection from the Member States. This could contribute to a network alert regarding critical structures (Critical Infrastructure Warning Information Network - CIWIN). The network was already put into operation in 2005. The main function of the network is to contribute in promoting the exchange of information on common threats and vulnerabilities and to ensure an exchange of appropriate measures and strategies that would reduce risk and protect critical infrastructure. EPCIP program helps states, critical infrastructure owners and users. In this respect, the European Committee for Standardization and other standardization bodies support network (CIWIN) and propose uniform safety standards suitable for all sectors concerned.

II.4 THE CRITICAL INFRASTRUCTURE PROTECTION LIFE CYCLE

The Critical Infrastructure Protection policy is not limited to securing an immediate and effective response in case of disruption. On the contrary, there are widely recognized phases in the CIP cycle combing prevention and cure. More specifically, governments and private parties involved should make sure that effective policy measures are in place for prevention and early warning, detection of major threats, risks and vulnerabilities. When a major failure occurs, measures should be in position to ensure a timely reaction and efficient crisis management.

For a good understanding of the critical infrastructure protection process let's imagine a cycle of six main phases, occurring before, during, and after an event that may compromise or degrade the infrastructure. These six phases build on one another to create a framework for a comprehensive solution for infrastructure assurance. They are structured as follows:

Phase 1. *Identification and evaluation.* The identification and evaluation phase is the foundation and most important phase of the CIP life cycle. This phase identifies the assets or functions that are absolutely critical and determines the assets or the functions vulnerabilities, as well as their interdependencies, configurations, and characteristics. An assessment is then made of the operational impact of infrastructure loss or degradation.

Phase 2. *Establish defense system.* This phase involves precautionary measures and actions taken before an event occurs to fix the known vulnerabilities that could cause an outage or compromise a critical infrastructure, asset or function. It may include actions like education and awareness, operational process or procedural changes in order to eliminate vulnerabilities.

Phase 3. *Indications and warnings*. The indications and warnings phase involves monitoring to assess the mission assurance capabilities of critical infrastructure assets and to determine if there are event indications to report. Indications are preparatory actions that indicate whether an infrastructure event is expected to occur or is planned. Indications are based on input at the tactical, operational, and strategic level. At the tactical level, input comes from asset owners. At the operational level, input comes from the critical infrastructure sectors. At the strategic level, input comes from intelligence, law enforcement, and the private sector. Warning is the process of notifying asset owners of a possible threat.

Phase 4. *Mitigation*. The mitigation phase comprises action taken during the event in response to warnings or incidents. Critical asset owners, critical infrastructure sectors and military operators take these actions to minimize the impact of event.

Phase 5. *Incident response.* This phase comprises putting in practice the plans and activities in order to eliminate the cause or source of event.

Phase 6. *Reconstruction*. The reconstruction phase involves action taken to rebuild critical infrastructure after the event.

Figure 3. Phases of the CIP life cycle.

CONCLUSIONS

Managerial approach of critical infrastructure protection is a necessity and a challenge at national, European and global level.

Critical infrastructure protection is an important well defined domain, at the intersection of several specialties such as security and national defense, civil emergency management, risk management, defense against disaster, crime and terrorism prevention and ensuring public safety and order

Critical infrastructure protection at this stage of its development is a new direction for global security, while also representing a significant step in its historical evolution.

Vulnerability assessment of critical infrastructure elements play a role of fundamental importance in determining the critical points that must be protected and further resources to be invested in it. Risk identification is also a key element in ensuring the protection of critical infrastructure in order to build an efficient defense system.

Establishing a public-private partnership provides an efficient and coherent framework, in accordance with the common responsibilities of the two sectors in the field under discussion.

Analysis of the relationships of the management of critical infrastructure protection revealed that managerial act in this area is functional development cycle with maximum or minimum discontinuity, where all functions are interconnected.

In order to fulfill the fundamental purpose of management of critical infrastructure protection (ensuring the flow of goods and services generated by the critical infrastructure for the smooth functioning of the state or community) total quality management can be considered the basic method of critical infrastructure protection management for organizational entities responsible in this regard.

Detailed knowledge of the risk level of each element of the critical infrastructure will facilitate choosing the most effective option for intervention in accordance with its features and characteristics of the environment.

In social practice it becomes mandatory to establish the most effective organizational mechanism to insert all elements consistently witch define implementation strategy in the field: policy, protection programs, emergency plans and standard operating procedures.

REFERENCES

1. E. Brunner and M. Suter - *International CIIP Handbook* 2008/2009;
2. Bernhard Hämmerli, Andrea Renda - *Protecting Critical Infrastructure in the EU*, 2010
3. Grigore Alexandrescu, Gheorghe Văduva - *Infrastructuri Critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* Editura Universităţii Naţionale de Apărare „Carol I" Bucureşti, 2006 ;
4. Ivo Bouwmans, Margot P.C. Weijnen, Adrian Gheorghe - *Infrastructures at Risk*, 2006;
5. Roberto Filippini (European Commission Joint Research Centre) - *Presentation at the second meeting of the CEPS Task Force*, CEPS, Brussels, 2006
6. Kenneth Neil Cukier (The economist) - *Ensuring (and Insuring?) Critical Information Infrastructure Protection,* 2005
7. Traian Băsescu - *Romania`s National Security Strategy,* 2007
8. *The American Heritage Dictionary of the English Language, Fourth Edition*
9. *Dictionary of Military and Associated Terms. US Department of Defense,* 2005
10. *European Council Directive,* 2008/114/CE
11. "*What is critical infrastructure?",* (www.ag.gov.au/agd)
12. *"About Critical Infrastructure", Public Safety Canada,* (www.ps-sp.gc.ca)
13. *"Critical Infrastructure Protection in Germany", Federal Office for Information Security,* (www.bsi.de)
14. *"Protecting the Critical National Infrastructure",* (www.security.homeoffice.gov.uk)
15. *"United States National Infrastructure Protection Plan",* (2006) (www.dhs.gov)
16. www.ceps.eu

PERFORMANCE CRITERIA FOR EVALUATING MANAGERIAL POSITIONS IN THE PENITENTIARY SYSTEM: *FROM THE CLASSICAL APPROACH TO THE MODERN PARADIGMS*

Prison commissioner Ştefan Horia CHIŞ

CONTENTS

INTRODUCTION

Prison fundamentally represents an axiological-social and institutional point of reference in any state and democratic society. Its communitary efficiency and relevance indicate the value and convenience of the criminal law within a certain interval of time; they also show the consistency and sustainability of governmental strategies of development specific to this domain, strategies promoted by the executive policymakers. Last but not least, they indicate the quality and professional performance generated by the human resources involved in maintaining and developing the prison administration.

Referring to the present Romanian prison system from an analytical and assessing perspective, we identify as essential vector its strategic-institutional placing in an intense stage of development and harmonization with the European and North-American standards regarding the law, infrastructure, procedures, management and operations.

Global management of Romanian prisons has recently undergone some strong, substantial and irreversible changes, starting with the staff, continuing with the resizing and modernization of the organization and a new criminal law, ending with efficient human resources policies.

However, the innovative character of these changes, of the law and management evolution, has not benefited of infrastructure development and symmetric financial support granted to the progress needs of local prison administrations which, in most cases, are poorly equipped and have less employees than necessary and also have low capacity of norms' absorbtion and implementation of new standards in the execution of custodial sentences.

The management of prisons, namely the quality and efficiency of the administration of the units that make up the national prison system, is currently a topic of operational implementation, teaching reflection and normative limitation, real progress being noted in defining clear criteria of evaluation of the management that is specific to this field.

The present paper aims to develop an integrated analysis of the evaluation system used for the positions with managerial responsibilities from the Romanian prison system; it also aims to make a comparison between the present formal criteria (provided by the statutory law of the personnel working in public prisons) and the

non-formal criteria (prevalent and commonly used in professional evaluations specific to this field) and provide a synthetic overview regarding the implementation of the criteria of modern European and North-American management (for example, the balanced scorecard).

The goal of the present paper is to emphasize the principles and procedures necessary to implement the modern external paradigms of evaluation of the professional performance associated to the manager position in the Romanian prison system.

According to the law[1], any strategic plan of an institution includes, as essential dimension, the management, with the following components:

- mandate – expresses the essential role of the institution within the public administration, as well as the social functions and the specific responsibilities;
- vision – describes the aspirations referring to the managerial goals specific to the institution, according to the defining material competences;
- common values – reflect the essential axiological landmarks which are accepted and undertaken by all employees;
- SWOT internal analysis (strenghts, weaknesses, opportunities, threats)
- PESTLE external analysis (political factors, economical factors, socio-cultural, technological and legal factors, the environment)
- medium term priorities – summarizes the objectives and the managerial activities;
- directions of activity – targets the main institutional policies addressed actively and consistently;
- monitoring, evaluation and reporting.

The fundamental law[2] which regulates the activity of the civil servants with special status in the prison system establishes the evaluation of the managerial responsibilities associated to the leadership position based on setting the level and quality of exercising the professional criteria (further details).

[1] Government Decision no.1807/2006 for the approval of the Management component within the Methodology regarding the system of strategic planning on medium term for the central public administration institutions.
[2] Law no. 293/2004 referring to the Status of the civil servants in the National Administration of Prisons, amended and supplemented.

I. ROMANIAN EVALUATION PATTERN FOR MANAGERIAL POSITIONS IN THE PENITENTIARY SYSTEM

1. Principles of management

From the perspective of the manager position in the prison system, we identify the following general principles, listed in the statutory law:

a) complete obedience to the law;

b) respecting the inmates' rights, according to the law;

c) equality of chances, based on merit and professional ability;

d) responsibility and impartiality;

e) efficiency, serving the general interests of the society;

f) efficiency in using resources;

g) organizational and functional hierarchy.

A specific and inductive approach of the priciples of public management is proposed by a well-known author[3], who describes them in a synthetic and correlated way:

Principles of public management

LEGALITY	The legal framework within which the activity takes place.
RESTRUCTURING	The goal: to create an efficient administrative body.
FLEXIBILITY	Adapting quickly to changes.
TRAINING	Required by the constant changes.
AUTONOMOUS MANAGEMENT	Adapting the system to time and place conditions – is combined with unitary management in order to avoid bureaucracy.
UNITARY MANAGEMENT	Subordination of government institutions to each other – well-defined hierarchy.

The current situation identified in the prison system, regarding the general topic of this paper, is characterized by the absence of some objective, explicit and

[3] Marinescu, P.: *Management of Public Institutions*, Bucharest University, Bucharest, 2003: http://ebooks.unibuc.ro/StiinteADM/marinescu/2.htm#5.

extensively specified criteria referring to the evaluation of the managerial performance.

Thus, the managerial instruments elaborated by the experts from the Ministry of Justice[4] correctly identify this major shortcoming and propose as specific objective to create the conditions for a performance management, at the level of the National Administration of Prisons, by designing and implementing an evaluation framework for managers, in accordance with their professional performance. In this respect, there is a proposal to develop an evaluation system for the central and individual management, as well as a set of rules regarding the minimum quality standards to be fulfilled by managers, which should generate, as key result, an objective evaluation of this type of personnel.

Quality management in public administration includes its reporting and efficiency as fundamental principles[5]. From this perspective, we mention the importance of implementing the Quality Management System in the Institutions of the Public Administration, based on the recommendations of the Standard ISO 9001:2000.

2. Instruments of management improvement and evaluation

A strategic objective involved in making the prison an efficient institution is the promotion and development of a modern management, that is scientifically validated, strategic, participatory and accountable, implemented and operationalized through the following elements:

- Consultation of the persons that are the object of a decision with the aim of establishing understading and real consent of these persons towards the subsequent meanings and consequences;
- Making the personnel responsible of achieving some professional goals, associated with the internalization of the needs and values involved, in order to eliminate the execution of tasks without adding extra individual value.

[4] Action plan to make the prison system more efficient 2008-2009: http://www.just.ro/Portals/0/plan%20de%20masuri%20anp_13112008.doc.

[5] Government Decision no. 1807/2006 for the approval of the Management component within the Methodology regarding the system of strategic planning on medium term for the central public administration institutions.

- Implementing the principle of subsidiarity in the sense of delegating operational decisions at the first level of competence allowed;
- Encouraging and favoring the reduction of inflexibility in administrative relations, both vertically (in terms of information flow) and horizontally (regarding coordination of actions).
- Implementing the rule of the 4Cs [6] :

- coherence:

a. of declarations and actions;
b. of decisions;
c. of objectives and means;
d. of evaluations;
e. of information transmitted within the organization;

- courage:

a. psychological and moral;
b. of decision;
c. in relations;

- clarity:

a. of the missions of the organization;
b. of the internal rules;
c. of the strategic options;
d. regarding exposure to risks and threats;
e. of results obtained;
f. of internal and external communication;

- considering:

a. each civil servant individually;
b. collaborators' work for periodical evaluation;
c. subordinates' ideas and proposals;

- personalized answers from the administration, adaptated to the comprehension skills of the recipient;
- simplicity and predictability of administrative approaches and procedures;

[6] Hintea, C.E., Ghioltan, C.: *Strategic Management in Public Administration*, Gewalt, Cluj-Napoca, 2000, p. 15.

- fast problem solving and solutions generated unequivocally.

Strategic management defines the fundamental orientations of an administrative organization or institution and its applied component is expressed through techniques of strategic management (TSM), which offer operational sustainability for these essential administrative orientations. In order to put into practice the theoretical approaches, the prison manager will have to develop and present, within the institution he is running, the following[7] :

- **managerial project**, which includes these basic components:
  - the future of the local prison, according to the social values and tasks undertaken;
  - internal processes underlying the development and operational construction of the prison objectives;
  - the documents developed for the prison, referring to the privileged values, strategic axes, action plans and communication plan;
- **tasks-defining letter**, so that the organization understands the role and responsibility of the manager, showing his clear attitude, a prospective vision of nature and an extension of his involvement in the effort to balance, transform and re-form the prison (eg. the nature and level of management, deadlines for tasks, setting up the objectives, ways to perform tasks, limits of competence);
- **the plan of activity**, as the annual procedure of operational planning, targets:
  - a prospective stage which announces the priorities of the prison for the year in progress;
  - to define the necessary actions according to the exact and measurable outcomes that have to be achieved;

[7] Hintea, C.E., Ghioltan, C.: cited work, p. 39.

- the efficient management of human, financial, technical and information resources;
- to promote an innovative management of the prison, characterized by a superior level of technical and relational expertise;

➢ **strategic plan of training personnel**, which is developed upon making a specific analysis of individual and collective needs, in order to improve professional expertise and communication abilities; the plan also states the forms of evaluation of the performance obtained and of the professional training opportunities, so that the professional abilities of the staff will increase and unequal access to training is reduced;

➢ **the management control** represents all means put in practice by the prison manager, as the representative of the public organization, in order to support the operational managers in the ongoing evaluation of the degree of achievement of objectives and the efficient use of the available resources. The manager's efficiency confers viability and relevance to the organizational efforts, as well as the ascendancy of the economic reasoning subsumed the management. The manager should act continuously and offer the personnel professional feedback that is relevant and stimulating.

Strategic planning, the main component of strategic management, sets the direction, the priority objectives and it is oriented towards accomplishing the standards of institutional efficiency[8]. At the same time, the prison manager must pay particular attention to his most important strategic task, namely the anticipatory task, with three essential components[9] :

- multi-level **prognosis** of the institution, on determined periods of time, whose validity and efficiency is expressed by the final degree of concordance between the reality of the areas and the evaluated variables (eg.: the evolution

[8] Cornescu, V., Marinescu, P., Curteanu, D., Toma, S.: *Management – from Theory to Practice*, Bucharest University, 2004 http://ebooks.unibuc.ro/StiinteADM/cornescu/cap3.htm.

[9] Ormenişan, G.: *Prison Management*, Europrint, Braşov, pp. 30-31.

of the number of inmates according to conditions of sentence execution, configuration of accommodation, level and rhythm of budgetary allocation of financial resources and of prison's own income etc.);

- **planning**, which consists in formulating general, derived and specific objectives, the way to mobilize and value the material, financial and human resources, in accordance with the activities carried out, managerial methods and techniques employed;
- **setting the schedule**, the essential dimension that makes the first two components operational; divided in a measure plan, actions structured on activity areas, resource allocation, managerial approaches, tasks and people who are responsible of them, reference period, deadlines, evalation indicators.

In order to have more responsible personnel and to involve them in making the activities more efficient, the prison manager will state clear and articulate decision-making levels in the prison and associated material competences, according to the following hierarchy:

1. tasks execution (surveillance and security agents, escorts, technical and logistic agents);
2. operative management (shift leaders, chiefs of operating points, deputies of shift leaders);
3. tactical management (head of office, head of service);
4. specialized-strategic management (deputy manager);
5. general-strategic management (manager).

The evaluation of employees' performance represents one of the most important managerial actions, with impact on the organization, as a few specific criteria[10] must be met at the same time:

- validity;
- exactness;
- objectivity.

[10] Burloiu, P. : *Human Resources Management*, Lumina Lex, Bucharest, p. 596.

At present, in the system of prison administration, the evaluation of professional performance is made every year, according to an evaluation sheet, which no longer meets the requirements of a modern and complete determination of the potential, abilities, professional and moral conduct of the civil servant with special status, manifested in the evaluated reference period; thus, we conclude these evaluation criteria must be changed.

3. Normative standards of competence in management

The statutory rules regulating matters related to the performance standards of management (Law no. 293/2004 referring to the Status of the civil servants in the National Administration of Prisons, amended and supplemented, republished) establishes the following criteria and sub-criteria for the evaluation of the management:

1. **Efficient organization**

Evaluation criteria:

- adequate and efficient use of human, material and financial resources;
- avoiding loss;
- evaluation of necessities;
- crisis management;
- relation investe resources – obtained results;
- information management;
- organizing professional training;
- distributing tasks.

2. **Behaviour and communication**

Evaluation criteria:

- behaviour and communication with subordinates, inmates, other persons or institutions the manager is in contact with, as well as with the mass-media;
- ensuring access to public information;
- transparency of management.

3. **Taking responsibility**

Evaluation criteria:

- fulfillment of duties stipulated by the law and regulations;

- implementation of national and sequential strategies in the field;
- the way in which the inmates' rights are respected as well as the other legal regulations regarding the execution of sentences.

4. Managerial skills

Evaluation criteria:

- ability to organize;
- ability to make decisions fast;
- resistance to stress;
- self-training;
- ability to analyze, synthesize, capacity of prevision, strategy and planning on short, medium and long term;
- initiative and ability to adapt fast.

Unfortunately, additional legislation does not include any legal provisions that stipulate measurement scales, standards and quantification parameters, namely inductive values, thus the decision-makers being the ones who decide, in a subjective way, the criteria applied to the professional performance and, as a consequence, there is a significant risk to associate value judgments with wrong decisions.

4. Non-formal criteria in management evaluation

In the management evaluation practice there are many criteria, established and well-known in the specialty literature, criteria with a significant prevalence, but which are not formalized as norms. The evaluators in the prison system consider these criteria as being fundamental in the process of evaluation of performace associated with different levels of management, as follows:

4.1. Physical environment and implementation of the penitentiary regime

One of the classical and general criteria of management quality evaluation is represented by the physical environment, seen as all the general ambient conditions for the activities in prison, either we refer to the standards imposed by the criminal law for the inmates or we take into consideration the characteritics of the environment in which the prison staff operates.

From the point of view of the conditions in prison and the way the sentence of deprivation of liberty is applied, the persons that are in provisional detention

(preventive arrest) or determined detention (convicted), the prison manager (at operational level) and the manager from the centre (strategic level) must design maintenance policies, infrastructure development and application of the prison regime, which should correspond to the specific regulations of internal law[11], as well as to the European recommendations and those coming from the international organizations competent in this field[12] , especially regarding:

- the accommodation of inmates;
- arranging and equipping detention rooms;
- ensuring conditions for individual and collective hygiene;
- the safety systems and vigil lighting;
- the equipment of inmates;
- feeding inmates;
- execution regimes of custodial sentences;
- the rights of the inmates;
- the work performed by inmates;
- the educational, cultural, therapeutic, psychological counselling, social assistance activities, school education and professional training for inmates;
- obligations and interdictions for inmates;
- rewards, misconduct, disciplinary offenses compense;
- contact with the outside;
- internal rules and daily schedule.

Complementary to any philosophy and operationalization of the principles of executing custodial sentences, a good prison manager will also concentrate on the prison staff, the working conditions, the training of the personnel, the real improvement of the professional performance and on maintaining a professional working environment with proper conduct, that is controllable and accurate from the evaluative perspective within which the components of integrity, professionalism and humanism are clearly defined and implemented.

[11] 1.Law no. 275/2006 referring to the Execution of sentences and measures ordered by the Court in criminal proceedings (Official Register of Laws of Romania no. 627 from 20.07.2006); 2. Government Decision no. 1897/2006 for the approval of the Implementing regulations for Law no. 275/2006 referring to Execution of sentences and measures ordered by the Court in criminal proceedings.

[12] 1.European Council – Committee of Ministers: Recommendation of the Committee of Ministers of the member states regarding the European Prison Rules REC (2006)2 – ANP, Bucharest, 2006; 2. United Nations Organization: Universal Declaration of Human Rights – International documents regarding the defence of human rights, ANP, Bucharest, 2003; 3. United Nations Organization: Standard minimum rules for the treatment of inmates – International documents regarding the defence of human rights, ANP, Bucharest, 2003.

4.2. Decency and humanism

Decency and humanism, internalized and assumed axiologically, unconditionally promoted and defended, effectivelly and continuously, constitute professional, human and Christian values that characterize the wise and performant manager.

This category of values represents the fundamental axis of the prison manager from the perspective of the inmates, who are deprived, legally and socially necessary, by the supreme property of the human condition: freedom.

The humanism principle in executing the custodial sentence represents an axiological landmark present in all national and international standards, consituting a *sine qua non* obligation of all prison administration and an obligation generally opposable to institutions involved in administration of criminal law.

Well-known authors in the field of prison phenomenology[13] consider that, in a morally justified and rationally argued way, one of the primary functions of the prison is the educational and therapeutic one.

In the opinion of the same author[14], respecting the rights of the inmates and preserving the fundamental values referred to above, depend on a real control of the prison, objectified in complementary forms, progressively interconnectd and integrated:

- administrative control;
- judicial control;
- control exercised by non-governmental organizations;
- control made by mass-media.

4.3. Organizational culture and better communication

Another main component of a performance consists in the proper management and use of the positive vectors of the institution and, last but not least, in the intelligent and timely promotion of good communication with mass-media and the community.

a. Organizational culture aspects

[13] Florian, G.: *Prison Phenomenology*, Oscar Print, Bucharest, 2003, p. 29.
[14] Florian, G.: *Prison Dynamics – Reform of Internal Structures*, Oscar Print, Bucharest, 1998, pp. 64-65.

The organizational culture includes all composite elements which allow the members of the institution to live together, communicate, work together and evolve professionally according to the general and specific objectives of the institution, expressing itself under the form of collective standards of thinking, specific rules and customs, thus fulfilling two reference functions:

- it is an essential factor of internal cohesion;
- provides an efficient and specific way to adapt to stress and external challenges, generating methods and positiove solutions to solve the problems.

In terms of components, the organizational culture is based on apparent manifestations, reference values and basic social postulates. Organizational cultures are not likely to make radical value judgments, in the sense that they cannot be divided into ”good” or ”bad” ones. They show a profound micro-social reality which shoud not be diverted from its basic sense and characteristics, its use being appropriate and efficient by real actions that can change the way it may increase the cohesion and efficiency of the institution through:

- the systematic use, adapted to the strenghts of the organization;
- determining its evolution by identifying and using the aspects that were advantages, but which, at present, are weak or vulnerable points.

b. Better communication

A priority approach of a prison manager should be the recovery, rebalancing and development of the relation with the local community and mass-media, to cover the deficit and consolidate in a real and transparent way the position of the prison within community, in concordance with the principles of institutional transparency and responsibility, by promoting a proactive policy and a intelligently planned relation with the mass-media and the community, by:

- promoting the activities of the prison within the community;
- developing cooperation relations with the local representatives of the state institutions and with the civil society;
- increasing the transparency of the institution, reforming and improving communication;
- professional crisis management;

- promoting the characteritics and risks of the profession of civil servant in prison;
- ensuring free access to public information;
- the activity of spokesperson should be considered a profession;
- periodic quality analysis and extension of the media impact in terms of prison work;
- prospective activities meant to identify possible social partners or cooperation opportunities.

As far as the internal communication is concerned, there have to be established clear rules and standards, which should regulate the relations between:

- civil servants, vertically and horizontally;
- civil servants and inmates.

It is also necessary to stimulate:

- employees' cohesion;
- the consolidation of the organizational culture;
- knowing the employees and helping them to have a positive state of mind;
- effective communication between employees, including thorugh new methods and communication channels.

For a final plastic and incidentally metaphysical approach, we render the opinion of a well-know prison-environment psychologist, who considers that the lack of communication generates meditation and feeling of guilt from the inmate and the dialogue is the only way to survive in detention[15].

Efficient communication, strategically planned by the prison manager, sustains the relation of the prison with the community and promotes its social values and the image of an important public organization, with the ethic substance of its identity of fundamental social service.

[15] Florian, G.: *Prison Psychology*, Oscar Print, Bucharest, 1996, p.16.

4.4. Treatment of visitors

The way of treating visitors is an institutional issue which a prison manager has to deal with professionally and differently, according to the type and quality of the persons who can legally benefit of access in the prison.

The prison manager who wants to promote a performing relationship management must understand that the community around the prison is an important objective of the efforts of axiological redefinition and confirmation of the social role, starting from the feeling of personal and social security, which the prison should offer to the citizens, and ending with the certainty that the custodial environment offered by this public institution is one of proper conduct, according to the regulations related to the human rights.

Thus, the relationship with the representatives of the community must be within general terms of responsibility, transparency and humanism, noting that the people who visit inmates must undergo a rigorous specialized control, according to the regulations, so that the order, discipline and security are maintained in the prison and also in order to prevent the introduction of prohibited objects.

In other words, the management of the relationship with the visitors must be extremely flexible and contextualized, harmoniously combining the transparency and assertiveness of an institution, deeply attached to the values of the community and the democratic society, with the rigors and operative procedures specific to the defense system, public order and national security the prison is part of.

The prison manager must promote a good image of the institution, generated by the correct and appropriate treatment of the visitors, but he must also maintain the security standards at the highest level in what concerns the access in the prison, the specialized and anti-terrorist control for the visitors who might be dangerous in this respect.

Concluding, we can state that the managerial activity that states the treatment applied to visitors depends on the healthy way of organizing[16] the prison and the adequate social image of the institution.

[16] Florian, G.: *Prison Phenomenology*, Oscar Print, Bucharest, 2003, p. 192.

4.5. Reaction under stress

One of the main and undisputed evaluation criteria is the manager's reaction under stress and, last but not least, the way he communicates his reaction inside and outside the prison.

Due to its very special characteristics, the prison is an environment signifiantly saturated by complex stress factors manifesting themselves in substantial doses, with a high pathogenic potential and maximum risk of generating maladaptative reactions from the prison staff, which may stimulate each other and thus maintain and enhance the deviant attitudes of the inmates

In this context, the prison manager is always subject to overexposure to multi-valent stress factors, either general[17] or specific, especially related to the institution: :

1. **general stress factors for the manager:**
   - ✓ responsibilities towards the superiors;
   - ✓ the necessity to motivate subordinates;
   - ✓ meeting deadlines;
   - ✓ respecting the budget;
   - ✓ adopting changes;
   - ✓ word overload;
   - ✓ difficulties in making decisions;
   - ✓ media exposure;
   - ✓ the quality of image vector of the institution;
   - ✓ general professional and public responsibility;
   - ✓ hierarchical temporality that is clearly stated (period of the mandate).
2. **specific stress factors:**
   - ✓ pathogenic prison environment;
   - ✓ solving conflicts within the institution that are frequently caused by the personnel, due to the closed, pathogenic and prohibitive work environment;
   - ✓ significant resistance to change and progress of the prison personnel, due to monotonous and rigid work;

[17] Deaconu, A., Podgoreanu, S., Rasca, L.: *The Human Factor and the Organization's Performance*, ASE, Bucharest, 2004: http://www.biblioteca-digitala.ase.ro/biblioteca/pagina2.asp?id=cap7.

- ✓ limiting psychological and axiological transfer from inmates to members of the staff;
- ✓ proper management of the relationship between the inmates and the members of the staff;
- ✓ precarious infrastructure of detention space and minimum technical and material equipment and facilities;
- ✓ ensuring the rights of the inmates despite the chronic underfunding and the subtantial gap between the legal requirements and the resources;
- ✓ the specific legislation is weak and ambiguous, denying the manager the access to fundamental managerial levers.

Besides the classical reactions to prison stress (physiological, psychological, behavioural), as a category (form) of distress and control techniques deployed in this respect, the prison manager must develop a personal plan with anti-stress strategies that are scientifically validated and adapted to his personality; these strategies should generate real internal controllability as well as maintain and even increase the level of managerial performance.

5. Current trends in establishing management evaluation criteria

In the last years, well-kown specialists in the domain of human resources and professional training, from the National Administration of Prisons, have developed different working variants referring to the evaluation criteria of the performing prison management, criteria which will be assumed, stated as norms and implemented in the professional period evaluation.

The next step in building an integrated and reliable system of management evaluation, based on recognized scientific criteria adapted to the particularities of prison administration and central structure, is represented by the audit of the management development[18], equivalent with a profound analytical approach towards management development activities, that will allow the superiors of the audited structure to identify the weaknesses and strenghts of the latter.

Thus, depending on the results of this complex management audit, a set of parameters and conclusions was released, underlying the new project of a Ministry Order (amending and supplementing the present Order of the Ministry of Justice no.

[18] Cole, G. A.: *Personnel Management*, Codecs, 2000, pp. 434-435.

2792/C/2004 for the approval of the Criteria regarding the evaluation of the performance in the professional activity of the civil servants from prison system and the judges assigned to the prison system); this new project offers a new and modern regulation of the evaluation of the staff from prisons, including the managers.

II. EUROPEAN AND NORTH-AMERICAN PARADIGM FOR ASSESSING MANAGERIAL POSITIONS IN THE PENITENTIARY SYSTEM

1. General theoretical aspects

Unlike the Romanian system of management evaluation which, although being based on good and valid general principles, does not provide measuring instruments standardized for an efficient evaluation of the professional performance, the European (with special emphasis on the well-known British system) and North-American prison administrations developed complex, evolved and valid paradigms to measure the level of management performance.

Thus, the managerial instruments promote measurability, standardization and validity of the evaluation, the results consisting of parametric quantification of the performance criteria to be evaluated and, consequently, they generate inductive value judgments, scientifically supported as far as the level of performance in prison management is concerned.

The American[19] presentation guides of the methods used to measure management performance expose in an accurate manner their role and characteristics, being generally opposable to all public institutions, including prisons.

According to these[20], a good performance measurement system should provide information that is meaningful and useful to decision-makers. A good system and good performance measures play an integral part in an agency's daily operations. An effective measurement system should satisfy the following criteria:

- **results-oriented: focuses primarily on outcomes, efficiencies, and outputs;**
- **selective: concentrates on the most important indicators of performance;**

[19] http://www.sao.state.ut.us/_finAudit/misc/Guide%20to%20Performance%20Measure%20Management.pdf
[20] idem

- **useful: provides information of value to the agency and decision-makers;**
- **accessible: provides periodic information about results;**
- **reliable: provides accurate, consistent information over time.**

The same American guides[21] distinguish between three main ways of measuring performance:

1. **outcomes (results/impact);**
2. **efficiency;**
3. **output (volume/effort).**

From this triple perspective, according to the same references[22] good performance measures should meet the following criteria:

- **responsive: reflect changes in levels of performance;**
- **valid: capture the information intended;**
- **cost-effective: justify the cost of collecting and retaining data;**
- **comprehensive coverage: incorporate significant aspects of agency operations;**
- **relevant: logically and directly relate to agency goals, objectives, strategies, and functions.**

Focusing on our reference area, we notice that the British prison system[23] is supervised from the managerial point of view and it is interconnected with the probation system by a governmental agency specialized in management, called National Offender Management Service.

One of major concerns of the British Management Academy, technically applied at institutional and sectorial level, is the management accountability in the Prison Service, a reason for which one of the authors[24] considers that ”the key manager in the Prison Service is the governor’s governor”; therefore the evaluation of the prison governors is based on the degree of accomplishment of the objectives from the management contract an don the measurement of the values for the performance indicators established.

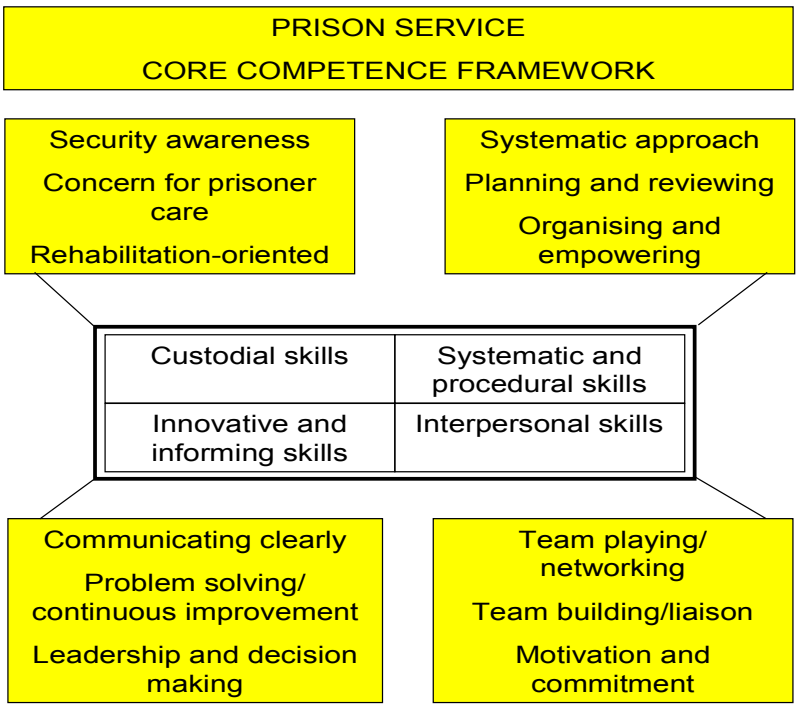
[21] ibidem
[22] ibidem 2
[23] http://www.justice.gov.uk/about/noms
[24] Train, C.J.: *Management Accountability in the Prison S*ervice, in the volume Prison Policy and Practice (collection Prison Service Journal), editors Reynolds, J. & Smartt, U., HMP Leyhill, 1996, pp. 153-154.

It is interesting to note that, despite the fact that the British and North-American prison systems have advanced technical instruments to measure performance, they do not ignore an essential dimension of the professional profile of the prison officer (especially of those with management responsibilities), namely the aspects that concern emotions and coping mechanisms.

It is well-known the fact that the prison is saturated with strong stress factors, as well as with deep emotional symbolism. A leading authority[25], with vast knowledge in the field of public and private aspects of the prison personnel, regards the prison as ”an emotional arena”, in which stress and emotions management[26] represents and important component in measuring professional performance in the prison system.

2. Core competence framework

In order to evaluate managerial performance in prison, it is necessary to define the main activity fields and their interdependencies. This is why we offer an illustrative example of British[27] origin, valuable through its relevance in relation with the institutional architecture of a prison:



Bryans, S. & Wilson , D.: *The Prison Governor – Theory and Practice*, HMP Leyhill, 2000, p. 195.

[25] Crawley, E.: *Doing Prison Work – The Public and Private Lives of Prison Officers*, Willan Publishing, 2006, p.130.
[26] Idem, p. 131
[27] Bryans, S. & Wilson , D.: *The Prison Governor – Theory and Practice*, HMP Leyhill, 2000, p. 195.

3. Key performance indicators

Key performance indicators define a set of values used to measure the performance in a quantitative way.

Each of the Prison Service objectives is supported by key performance indicators[28] (example):

- Prison Service Objective: to protect the public by holding those committed by the courts in a safe, decent and healthy environment;
- Key performance indicators (for this objective):

  - to ensure that the number of escapes from prison, and escorts undertaken by staff, expressed as a proportion of the prison population, is lower than 0.05%:

  - to ensure that the number of escapes from contracted out escorts is no more than 1 per 20,000 prisoners handled;

  - to ensure that the number of positive adjudications of assault on staff, prisoners and others, expressed as a proportion of the average population, is lower than 9%.

Another good example is provided by the official documents of HM Prison Service – Public Sector Prisons (UK)[29]:

1. *WORKING TO ACHIEVE RESULTS (COMPETENCE)*

1.A. Organizing and Maximizing Performance (OBJECTIVE)

Plans and supervision activities and resources to maximise performance (ACTIVITY)

ADDITIONAL INDICATORS FOR MANAGERS

[1.]First line management:

• Communicates how own team contributes to the overall priorities and business plan;

• Implements plans;

• Strives to ensure that targets are achieved;

[28] Idem, p. 162

[29] http://www.justice.gov.uk/downloads/jobs/hmps-competence-framework.pdf

• Systematically organises team activities;

• Makes best use of resources;

• Clearly informs the team as to their tasks and responsibilities;

• Sets clear standards, expectations and boundaries;

• Sets and agrees clear, realistic individual and team objectives that are specific, measurable, achievable, relevant and time bound (SMART);

• Obtains regular updates on progress against objectives:

• Manages risk associated with plans.

[2.]Middle management:

•Communicates how own unit contributes to the overall priorities and business plan;

• Ensures plans are implemented;

• Strives to ensure that targets, outcomes and benefits are achieved;

• Systematically organizes activities, clarifying tasks and responsibilities and making best use of resources; and ensures managers do the same;

• Sets clear standards, expectations and boundaries;

• Ensures clear, realistic, SMART individual and team objectives are set and agreed;

• Obtains regular updates on progress against objectives and ensures managers do the same;

• Ensures risks associated with plans are managed and mitigated.

[3.]Senior management

• Sets the vision and direction; communicates priorities and business plans; and ensures individual and team objectives are aligned with them;

• Delivers against plan and forecasts accurately;

• Defines targets, outcomes and benefits, and strives to ensure they are achieved;

• Systematically organises activities, clarifying tasks and responsibilities and making best use of resources; and ensures managers do the same;

• Sets clear standards, expectations and boundaries;

• Ensures that clear, realistic, SMART individual and team objectives are set and agreed across the establishment / unit;

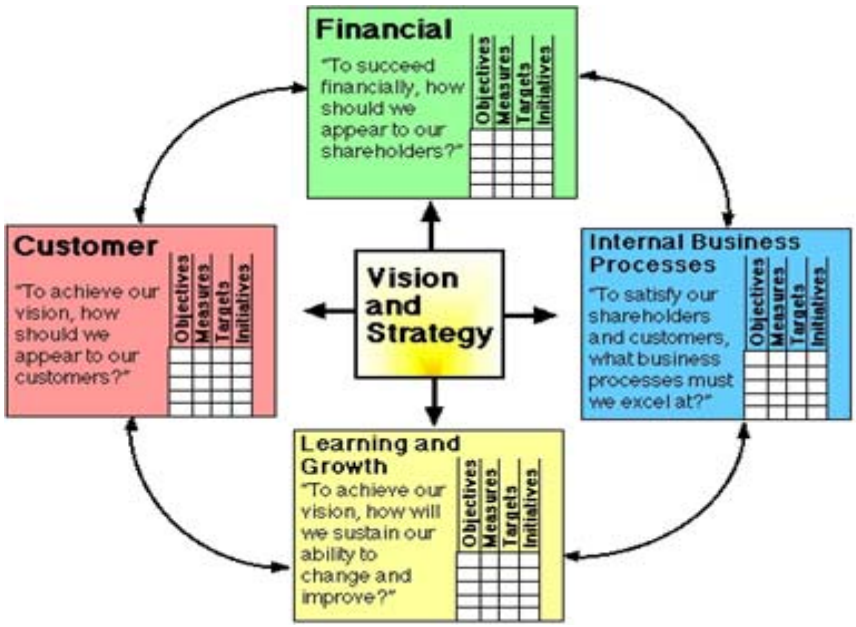
• Sets and influences stretching targets to improve value;

• Ensures progress is regularly monitored at all levels.

4. Balanced scorecard

The balanced scorecard translates an organization's mission and strategy into a comprehensive set of performance measures that provides the framework for a strategic measurement and management system[30].

The balanced scorecard has evolved from its early use as a simple performance measurement framework to a full strategic planning and management system[31]:



Adapted from Robert S. Kaplan and David P. Norton, *Using the Balanced Scorecard as a Strategic Management System*, Harvard Business Review (January-February 1996): 76.

Balanced scorecard measures have five essential components interconnected with the following meanings[32]:

- **Objectives** define how to satisfy your stakeholders' and customers' requirements for each Balanced Scorecard perspective;
- **Measures** define how to determine achievement of the objectives or progress toward the objective;
- **Definitions** are descriptions of the measure to ensure an understanding by everyone involved of what the measure represents;

[30] Kaplan, R.S. & Norton, D.P. : *The Balanced Scorecard: Translating Strategy into Action*, Harvard College, 1996, p. 2.
[31] http://www.balancedscorecard.org/BSCResources/AbouttheBalancedScorecard/tabid/55/Default.aspx
[32] http://www.doncio.navy.mil/uploads/1025WFC99792.pdf

- **Targets** are the desired value or limits on value of the measure or dimension of performance;
- **Actions** are defined as those steps that must be accomplished to achieve particular outcomes.

In the folowing lines we are going to present a contribution of the author, as a small applied modelling work, that represents a balanced scorecard type approach, used in the case of evaluating a prison manager:

Balanced scorecard

(a penitentiary approach)

OBJECTIVES	MEASURES	DEFINITION	TARGETS	ACTIONS
Improve the safety of prison (deadline: a year)	Numbers of escapes / 1 year	How many inmates escaped from prison or outside prison escort during one year	Number of escapes decrease with 50% compared to previous year	• Acquisition and implementing more security systems (eg: CCTV cameras, individual means for inmates' restraint, advanced cars for escorting); • Providing a better level of dynamic security by involving more inmates in work, educational and social activities; • Increasing the number of visits with family.
Reduce budgetary resources allocated to feeding inmates (deadline: 6 months)	Amount spent for 1 inmate/1 month	Calculating direct and indirect costs necessary for feeding an inmate in a month	Amount/1 inmate/1 month decrease with 20%	• Growth of prison's own income through more work contracted with inmates
Optimize professional training of prison officers (deadline: 3 months)	Evaluation test results	Determining the average of marks obtained by each officer at the subjects of examination	Percentage of officers who pass the exam at first test to grow 25% compared to previous assessment	• Mentoring • Training courses • Practical applications and simulation in their field of work.

CONCLUSIONS

The present paper conducted a synthetic and integrative inventory of the current institutional methods, either formal (established in the legislation) or non-formal, şi non-formale (arising from practice and academic approaches) to evaluate professional performance of prison managers in the Romanian prison system.

Regarding the Romanian model, we can conclude that, at present, beyond good, professional and ethical principles that are subsumed, there is no standardized, valid and objective system to measure and quantify professional performance that are the object of evaluation; therefore, there is the significant risk that the value judgments and the decisions inductively generated by these evaluations could be incorrect or disproportionate in relation with the reality.

In the final part, we presented comparatively, in a summary, for resons of limited extension of the document, a few of the most important and advanced paradigms in the field of measuring management performance in European (especially the British system) and North-American prisons.

The essential final conclusion of the paper indicates, in a demonstrated and exemplified way, the necessity to implement these competitive and modern systems of measuring managerial performance, of course inteligently adapted to the Romanian prison system (and why not to the whole public system), as the professional, institutional and strategic decisions of the prison manager must reveal competence and responsibility.

For any public institution, public or private, the correct evaluation, scientifically based on the performance of the managers, represents a major competitive advantage, that will generate progress, professional ethics and social prestige.

REFERENCES

1. Specialty papers

[1.] Burloiu, P.: *Human Resourcers Management*, Lumina Lex, Bucharest, p. 596.

[2.] Bryans, S. & Wilson , D.: *The Prison Governor – Theory and Practice*, HMP Leyhill, 2000, p. 195.

[3.] Cole, G. A.: *Personnel Management*, Codecs, 2000, pp. 434-435.

[4.] Cornescu, V., Marinescu, P., Curteanu, D., Toma, S.: *Management – from Theory to Practice*, Bucharest University, 2004 – http://ebooks.unibuc.ro/StiinteADM/cornescu/cap3.htm.

[5.] Crawley, E.: *Doing Prison Work – The Public and Private Lives of Prison Officers*, Willan Publishing, 2006, p.130.

[6.] Deaconu, A., Podgoreanu, S., Rasca, L.: *The Human Factor and the Organization's Performance*, ASE, Bucharest, 2004: http://www.biblioteca-digitala.ase.ro/biblioteca/pagina2.asp?id=cap7.

[7.] Florian, G.: *Prison Psychology*, Oscar Print, Bucharest, 1996, p.16.

[8.] Florian, G.: *Prison Dynamics – Reform of Internal Structures*, Oscar Print, Bucharest, 1998, pp. 64-65.

[9.] Florian, G.: *Prison Phenomenology*, Oscar Print, Bucharest, 2003, p. 29.

[10.] Hintea, C.E., Ghioltan, C.: *Strategic Management in Public Administration*, Gewalt, Cluj-Napoca, 2000, p. 15.

[11.] Kaplan, R.S. & Norton, D.P.: *The Balanced Scorecard: Translating Strategy into Action*, Harvard College, 1996, p. 2.

[12.] Marinescu, P.: *Management of Public Institutions*, Bucharest University, 2003: http://ebooks.unibuc.ro/StiinteADM/marinescu/2.htm#5.

[13.] Ormenişan, G.: *Prison Management*, Europrint, Braşov, pp. 30-31.

[14.] Train, C.J. : *Management Accountability in the Prison Service*, in volume *Prison Policy and Practice* (collection Prison Service Journal), editors Reynolds, J. & Smartt, U., HMP Leyhill, 1996, pp. 153-154.

2.National and international laws, specific normative recommendations and institutional documents

[1.] Law no. 293/2004 referring to the Status of the civil servants in the National Administration of Prisons, amended and supplemented, republished.

[2.] Law no. 275/2006 referring to the Execution of sentences and measures ordered by the Court in criminal proceedings, amended and supplemented, republished.

[3.] Government Decision no. 1897/2006 for the approval of the Implementing regulations for Law no. 275/2006 referring to Execution of sentences and measures ordered by the Court in criminal proceedings, amended and supplemented, republished.

[4.] Government Decision no. 1807/2006 for the approval of the Management component within the Methodology regarding the system of strategic planning on medium term for the central public administration institutions.

[5.] European Council – Committee of Ministers: Recommendation of the Committee of Ministers of the member states regarding the European Prison Rules REC (2006)2 – ANP, Bucharest, 2006.

[6.] United Nations Organization: Universal Declaration of Human Rights – International documents regarding the defence of human rights – International documents regarding the defence of human rights, ANP, Bucharest, 2003.

[7.] United Nations Organization: Standard minimum rules for the treatment of inmates – International documents regarding the defence of human rights, ANP, Bucharest, 2003.

[8.] Action plan to make the prison system more efficient 2008-2009: http://www.just.ro/Portals/0/plan%20de%20masuri%20anp_13112008.doc.

3.Institutional and governmental online resources

[1.] http://www.sao.state.ut.us/_finAudit/misc/Guide%20to%20Performance%20Measure%20Management.pdf

[2.] http://www.justice.gov.uk/about/noms

[3.] http://www.justice.gov.uk/downloads/jobs/hmps-competence-framework.pdf

[4.] http://www.balancedscorecard.org/BSCResources/AbouttheBalancedScorecard/tabid/55/Default.aspx

[5.] http://www.doncio.navy.mil/uploads/1025WFC99792.pdf

CURRENT NEED FOR THE TRANSFORMATIONAL STYLE OF LEADERSHIP

LTC Iulian CIOLAN, M.Sc.

CONTENTS

Introduction

There are various meanings of the word leader. Between the sense leader, there are interesting things to observe. Almost all of the meaning of the leader will always lead to a person who has influence over the ‘command’ who ‘instructed’ to the people around him who think he’s the leader.

The current environment characterized by uncertainty, global turbulence, and organizational instability calls for transformational leadership to prevail at all levels of the organization. The followers of such leaders demonstrate high levels of job satisfaction and organizational commitment, and engage in organizational citizenship behaviors. With such a devoted workforce, it will definitely be useful to consider making efforts towards developing ways of transforming organization through leadership.

1. Don’t hesitate to be a leader

Many CIOs are in a defensive mode. They feel like they’re under siege mode and fighting to stay alive from day to day. As a result, they tend to focus on protecting the status quo. That’s a mistake.

It’s far better to be proactive. Have a roadmap showing exactly where you plan to go. When you are the CIO, you cannot adopt a ‘wait-and-see’ attitude. You have to go in with a very clear and specific agenda of transformational change. You need to be moving away from the status quo, not presiding over it.

The life of a CIO can be difficult because IT operations often appear mysterious to outsiders. Even when senior executives don’t understand precisely how IT works, they understand that money is being spent, and they hold the CIO accountable when they don’t believe that IT is generating value.

Avoiding that scenario requires advance planning and preparation. The CIO has to be in the driver’s seat, setting the agenda and establishing realistic goals. Don’t let other people set the baselines. The CIO should be the one who declares victory.

Leveraging the cloud’s ability to provide “pay by the drink” infrastructure services can make it easier for CIOs to spend more time focusing on value creation, and less time worrying about keeping the lights on.

The amount of compute that has to be delivered to the world over the next 10-20 years is tremendous, and there aren’t enough system administrators and database administrators and network security people to manage that kind of

infrastructure model. So we have to go to a completely different model. For most CIOs, that means they're not going to be running infrastructure. It means they're going to be buying 'compute' the same way they're buying power, dial tone, and bandwidth – by the drink.

If the infrastructure goes away, what becomes of the CIO? If the infrastructure is behind the curtain then your focus is going to be internal delivery, work flow automation and really understanding how technology can change and affect the business in a way that the business actually notices. Instead of spending most of your time tending infrastructure, you're going to spend 90% of your time understanding how technology affects the business. That means your focus is at application level, not at the infrastructure level.

2. What is transformational leadership?

Creating high-performance workforce has become increasingly important and to do so business leaders must be able to inspire organizational members to go beyond their task requirements. As a result, new concepts of leadership have emerged - transformational leadership being one of them.

Transformational leadership may be found at all levels of the organization: teams, departments, divisions, and organization as a whole. Such leaders are visionary, inspiring, daring, risk-takers, and thoughtful thinkers. They have a charismatic appeal. But charisma alone is insufficient for changing the way an organization operates. For bringing major changes, transformational leaders must exhibit the following four factors:

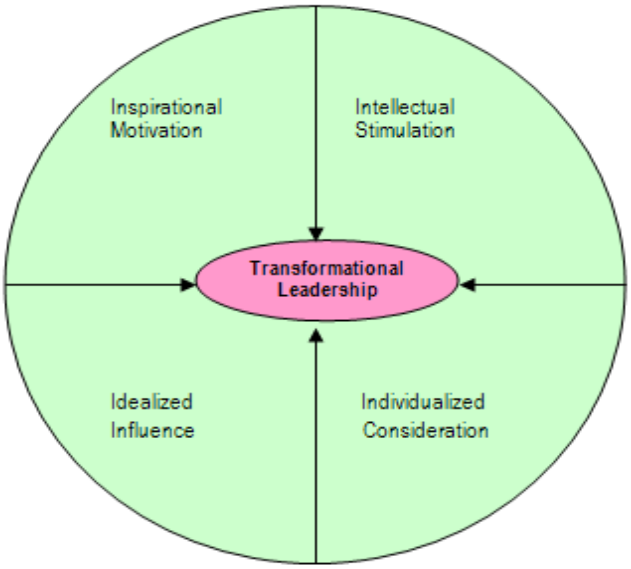


Figure 1: Model of Transformational Leadership

Inspirational Motivation: The foundation of transformational leadership is the promotion of consistent vision, mission, and a set of values to the members. Their vision is so compelling that they know what they want from every interaction. Transformational leaders guide followers by providing them with a sense of meaning and challenge. They work enthusiastically and optimistically to foster the spirit of teamwork and commitment.

Intellectual Stimulation: Such leaders encourage their followers to be innovative and creative. They encourage new ideas from their followers and never criticize them publicly for the mistakes committed by them. The leaders focus on the "what" in problems and do not focus on the blaming part of it. They have no hesitation in discarding an old practice set by them if it is found ineffective.

Idealized Influence: They believe in the philosophy that a leader can influence followers only when he practices what he preaches. The leaders act as role models that followers seek to emulate. Such leaders always win the trust and respect of their followers through their action. They typically place their followers needs over their own, sacrifice their personal gains for them, ad demonstrate high standards of ethical conduct. The use of power by such leaders is aimed at influencing them to strive for the common goals of the organization.

Individualized Consideration: Leaders act as mentors to their followers and reward them for creativity and innovation. The followers are treated differently according to their talents and knowledge. They are empowered to make decisions and are always provided with the needed support to implement their decisions.

Criticisms of Transformational Leadership Theory

•Transformational leadership makes use of impression management and therefore lends itself to amoral self promotion by leaders

•The theory is very difficult to be trained or taught because it is a combination of many leadership theories.

•Followers might be manipulated by leaders and there are chances that they lose more than they gain.

3. Is CIO a transformational leader?

The transformational CIO must inspire and motivate on the one hand and shove with the other. The key to IT transformation is to start with senior level company or divisional management and know just how far you can push.

If this approach sounds familiar, that's because "transformational leadership" has been around for decades. A 2004 analysis by Timothy Judge and Ronald Piccolo at the University of Florida and published in the Journal of Applied Psychology found that transformational leadership is nothing new. It tracks back to a similar style promoted in 1921. So, no, it isn't that the leadership style is new, what's new is CIOs have to do it ... not just CEOs.

For example, in healthcare the CIO "needs to be a leader, innovator and strategic thinker," said Mike Tucker, general manager PBM Products & Technology-Payer Solutions at IMS Health. This used to be just the CEO's job description.

He says the scale of healthcare reform is incredibly broad and the CIO needs to be constantly learning about regulatory and industry trends; looking for opportunities to advance critical areas of change. "In the past, the healthcare CIO has been a cost and project manager. The new healthcare CIO needs to be a thought leader as well as an operations expert."

These days, CIOs are not encouraged to be transformational leaders, they are expected to be. Further, transformation is expected to be delivered immediately and on-demand.

The transformational CIO has read the writing on the wall (in this case, outsourcing docs). He knows that IT jobs have fled overseas and he knows that his team knows this, as well. Therefore, the motivation to put the business' welfare over that of the IT department's is mostly absent. Yet, the CIO cannot muster change unless he can first rally his troops. The best way to do that is to eradicate the fear first.

While few CIOs can unequivocally promise no layoffs, nearly all CIOs can ease uncertainty by clearly presenting the team's actual circumstances and offering a means to successfully compete. Spell out to your teams that IT is increasingly being viewed as any other service provider to the business. This means they have to deliver end-user services (email, telecom etc.), business services (applications) and infrastructure (compute, storage, etc.) all the while being "price, quality and value comparable to external service providers" said Sunny Gupta, co-founder, president and CEO of Apptio.

The transformative CIO will have to manage their IT portfolio from a services perspective and measure on-going cost, value and quality of service. "Detailed, actionable metrics such as direct/indirect and fixed/variable will be favored over basic IT-specific measurements like utilization and performance. Only then will the CIO be

able to bridge the chasm that currently exists between IT and their business partners."

Once that chasm is bridged, the IT team and its CIO become invaluable to the business, not because of their technical knowledge, which can easily be replaced by outsourcers, but by their ability to form and hone the business' competitive edge. This becomes the IT team's formidable differentiator. The message to the IT team then is, "This is how you compete and win!"

4. The ABCs of transformational leadership

According to Bonnie McEwan, visiting lecturer in Management and Leadership, Milano The New School for Management and Policy in New York City, there are three key things a leader must focus on if they aspire to be truly transformational:

1. Always remember that the transformation is two-way : You will be changed along with your followers. Transformation is a process and its power lies in the exchange (and the changes) that take place between people.

2. Great leaders are also great followers : Transformational leaders know when to step back and let another take the lead. It is especially useful to embrace your follower role when you are seeking to develop the leadership abilities of others. Since leaders are at or near the top of the organizational hierarchy, it can be difficult to see what's really happening on the ground, where the work of your organization takes place. Followers often see realities that leaders miss, so it's important to allow your best followers to take the lead sometimes, and even encourage them to mentor you.

3. Be very clear about the transformation you seek: Know what it looks like, and describe it for your followers. This is more than just your vision. It's a shared view of a transformed reality that you all strive for together. Talk about the transformed reality every day, as that's what inspires people to move forward. Model that new reality in everything you say and do; make it tangible for your followers.

Indeed, bringing about transformation is a hands-on job. "The leader can't be a faceless name behind emails but must interact with the team frequently and with the members of the organization IT is serving," said Mike Honeycutt who has worked in IT for the University of North Carolina at Asheville for 28 years.

Yes, the transformational CIO must have a strong vision and be able to communicate it effectively to the team but that is the starting point not the end-point.

The CIO must possess an equal mix of charisma, business acumen, people skills, motivational ability, conviction, and courage. His commitment to the organization and the team must be unwavering and his knowledge of things outside IT forever growing.

5. 10 Characteristics of transformational leaders

There are certain core characteristics the majority of leaders possess. However, there are also an additional set of characteristics that define transformational leaders — leaders that have the ability to make an impact on organizational growth.

It is an organizations ability to develop this next level of leadership capabilities through training programs, mentoring, and skill development programs that put organizations in the enviable position to grow year over year without experiencing dips in performance.

Core leadership characteristics

There are certain leadership characteristics that, while important, do not inspire organizational change and growth that help companies develop into innovative, consistent industry leaders.

Examples of these core leadership characteristics include:

- Good judgment
- Communication skills
- Competence or knowledge
- Interpersonal skills
- Confidence

We hear about these leadership characteristics all the time and in many different contexts. While they are very important for leaders to have, there is another level of leadership characteristics that are “must haves” for transformational leaders. These are the leadership characteristics that make an impact and spur growth.

Transformational Leadership characteristics that impact organizational growth

In order to put your organization in a position to grow effectively and on a consistent basis, leaders with the following characteristics not only make them an effective leader — but also a transformational leader:

1. Internal motivation and self-management: Transformational leaders find motivation from within and use that as the driving force to effectively manage the

direction of the company. The best natural form of motivation is to love what you do and ensure that your values are aligned with the organization you work with.

2. The ability to make difficult decisions: Difficult decisions are a part of being a leader. Transformational leaders do not back away or put off tough decisions. Difficult decisions are made easier when decisions align with clearly defined vision, values, goals, and objectives.

3. Check their ego: When placed in a position of power, it is easy to let your ego get the best of you. However, transformational leaders keep their ego in check and do not let it get in the way of doing what is best for business. The benefit of checking your ego ensures you put the company first over personal gain and encourages the best input from others within the organization — because when the company succeeds, you as a leader also succeed.

4. Willing to take the right risks: Anyone can take a risk. Transformational leaders take calculated risks that more often than not result in positive outcomes. Trusting your instinct, as well as your team to gather the necessary intelligence is important. Trusting your gut is easier when you have taken the time to research, evaluate and inform your decisions with input from those around you. Failure to take the appropriate risks and make these difficult decisions will inhibit change and your ability to grow.

5. Organizational consciousness: Transformational leaders share the collective conscious of their organization. They understand what actions to take to evoke change, spur innovation, and make decisions that will create growth. Since their own values are aligned with the organization they share a joint purpose with the organization and do not just view their position in the company as just a job.

6. Adaptability: Transformational leaders are willing to adapt and are always seeking new ways to respond to a constantly changing business environment. They know that the second they stand still is when they will be passed by their competitors; which means they are open-minded to change and lifelong learners.

7. Willing to listen and entertain new ideas: It is a rare individual who can build an empire. Transformational leaders understand that success is a team effort and growth is derived from the willingness to be open and listen to ideas from all levels of their organization. Transformational leaders create intentional ways to listen to their team and incorporate their insights.

8. Inspirational: People want to be inspired. Transformational leaders have the ability to make those around rise to the occasion. Inspiration comes not just from

a formal motivational speech or simple recognition for a job well done, but by treating people as individuals and taking the time to understand what motivates and inspires their team.

9. Proactive: Transformational leaders are proactive decision makers. They do not wait around for others to make decisions and then react. They are willing to take risks, try new things and take an innovative approach to growing the organization. However, they also understand how to manage risk and make decisions that are backed by research, multiple insights and are well thought out.

10. Visionary: Being a visionary is about setting a realistic and concise company mission, vision, and values that fit the culture of your organization. Transformational leaders have the ability not only to effectively communicate the vision, but also get every person to buy in and work toward that vision by communicating with passion and clearly emphasizing the direction they want the company to pursue.

Transformational leaders constantly strive to have these characteristics. Developing these characteristics is what separates CIO'S that are managers versus leaders.

Conclusions

In conclusion, the merits of transformational leadership should speak for themselves. In light of the ambiguous strategic environment, it would appear to be obvious that most large organizations require leaders and followers steeped in the same core values and energized to tackle the tough issues together.

When leaders and led are on the same strategic page all their energy is focused to achieve maximum results with less oversight, because the leader has articulated the target goal so everyone understands the direction to move toward.

REFERENCES

1. http://www.cioupdate.com/career/article.php/3920606/Are-You-a-Transformational-CIO.htm

2. http://thetransformationalcio.com/1160/dont-hesitate-to-be-a-leader/

3. http://www.russellreynolds.com/content/cio-leadership-diagnostic

4. http://www.billhogg.ca/2012/03/10-characteristics-of-transformational-leaders/

5. http://www.amazon.com/Transformational-CIO-Leadership-Innovation-

6. http://blog.thehigheredcio.com/2012/04/30/what-is-transformational-leadership/

MEASUREMENT AND METRICS IN SOFTWARE DEVELOPMENT

LTC Emil ŞCHIOPU

CONTENTS

MEASUREMENT AND METRICS IN SOFTWARE DEVELOPMENT

INTRODUCTION

Poor size estimation is one of the main reasons major software-intensive acquisition programs ultimately fail. Size is the critical factor in determining cost, schedule, and effort. The failure to accurately predict (usually too small) results in budget overruns and late deliveries which undermine confidence and erode support for your program. Size estimation is a complicated activity, the results of which must be constantly updated with actual counts throughout the life cycle. Size measures include source lines-of-code, function points, and feature points. Complexity is a function of size, which greatly impacts design errors and latent defects, ultimately resulting in quality problems, cost overruns, and schedule slips. Complexity must be continuously measured, tracked, and controlled. Another factor leading to size estimate inaccuracies is requirements creep which also must be baseline and diligently controlled.

Any human-intensive activity, without control, deteriorates over time. It takes constant attention and discipline to keep software acquisition and development processes from breaking down — let alone improving them. If you do not measure, there is no way to know whether processes are on track or if they are improving. Measurement provides a way for you to assess the status of your program to determine if it is in trouble or in need of corrective action and process improvement. This assessment must be based on up-to-date measures that reflect current program status, both in relation to the program plan and to models of expected performance drawn from historical data of similar programs. If, through measurement, you diagnose your program as being in trouble, you will be able take meaningful, effective remedial action (e.g., controlling requirements changes, improving response time to the developer, relaxing performance requirements, extending your schedule, adding money, or any number of options. Measurement provides benefits at the strategic, program, and technical levels.

A good measurement program is an investment in success by facilitating early detection of problems, and by providing quantitative clarification of critical development issues. Metrics give you the ability to identify, resolve, and/or curtail risk issues before they surface. Measurement must not be a goal in itself. It must be integrated into the total software life cycle — not independent of it. To be effective, metrics must not only be collected — they must be used!

I. SOFTWARE ESTIMATION

Just as we typically need to determine the weight, volume, and dynamic flight characteristics of a developmental aircraft as part of the planning process, you need to determine how much software to build. One of the main reasons software programs fail is our inability to accurately estimate software size. Because we almost always estimate size too low, we do not adequately fund or allow enough time for development. Poor size estimates are usually at the heart of cost and schedule overruns.

The key to credible software sizing is to use a variety of software sizing techniques, and not to rely on a single source or method for the estimate.

Because accuracy can be improved if estimates are performed with smaller product elements, base your estimates on the smallest possible unit of each component.

It is absolutely critical that you measure, track, and control software size throughout development. You need to track the actual software size against original estimates (and revisions) both incrementally and for the total build. Analysis is necessary to determine trends in software size and functionality progress.

Software size has a direct effect on overall development cost and schedule. Early significant deviations in software size data indicate problems such as:

- Problems in the model(s), logic, and rationale used to develop the estimates,
- Problems in requirements stability, design, coding, and process,
- Unrealistic interpretation of original requirements and resource estimates to develop the system, and
- Faulty software productivity rate estimates.

Significant departures from code development estimates should trigger a risk assessment of the present and overall effort. Size-based models should be revisited to compare your development program with those of similar domain, scope, size, and complexity, if possible.

I.1. Measuring Software Size

There are three basic methods for measuring software size. Historically, the primary measure of soft are size has been the number Source Lines-of-Code (SLOC). However, it is difficult to relate software functional requirements to SLOC, especially during the early stages of development. An alternative method, function points, should be used to estimate software size. Function points are used primarily for management information systems (MISs), whereas, feature points (similar to function points) are used for real-time or embedded systems. SLOC, function points, and feature points are valuable size estimation techniques. Table 1 summarizes the differences between the function point and SLOC methods.

FUNCTION POINTS	SOURCE LINES-OF-CODE
Specification-based	Analogy-based
Language independent	Language dependent
User-oriented	Design-oriented
Variations a function of counting conventions	Variations a function of languages
Expandable to source lines-of-code	Convertible to function points

Table 1. Function Points Versus Lines-of-Code.

I.2. Source Lines-of-Code Estimates

Most SLOC estimates count all executable instructions and data declarations but exclude comments, blanks, and continuation lines. SLOC can be used to estimate size through analogy — by comparing the new software's functionality to similar functionality found in other historic applications. The most significant advantage of SLOC estimates is that they directly relate to the software to be built. Your estimates will need to be continually updated as new information is available.

A large body of literature and historical data exists that uses SLOC, or thousands of source linesof- code (KSLOC), as the size measure.

Because SLOCs are language-specific, the definition of how SLOCs are counted has been troublesome to standardize. This makes comparisons of size

estimates between applications written in different programming languages difficult even though conversion factors are available.

I.3. Function Point Size Estimates

Function points are the weighted sums of five different factors that relate to user requirements:

- Inputs,
- Outputs,
- Logic (or master) files,
- Inquiries, and
- Interfaces.

Function points are counted by first tallying the number of each type of function listed above. These unadjusted function point totals are subsequently adjusted by applying complexity measures to each type of function point. The sum of the total complexity-adjusted function points (for all types of function points) becomes the total adjusted function point count. Based on prior experience, the final function point figure can be converted into a reasonably good estimate of required development resources.

Like SLOC, function points too are affected by changes in system and/or software requirements.

II. SOFTWARE MEASUREMENT

You cannot build quality software, or improve your process, without measurement. Measurement is essential to achieving the basic management objectives of prediction, progress, and process improvement. An oft-repeated phrase by DeMarco holds true; “You can’t manage what you can’t measure!”. All process improvement must be based on measuring where you have been, where you are now, and properly using the data to predict where you are heading. Collecting good metrics and properly using them always leads to process improvement!

II.1. Measures and Metrics, and Indicators

A software measurement is a quantifiable dimension, attribute, or amount of any aspect of a software program, product, or process. It is the raw data which are associated with various elements of the software process and product. Table 2 gives some examples of useful management measures.

AREA	MEASURES
Requirements	• Computer software configuration item (CSCI) requirements • CSCI design stability
Performance	• Input/output bus throughout capability • Processor memory utilization • Processor throughout put utilization
Schedule	• Requirements allocation status • Preliminary design status • Code and unit test status • Integration status
Cost	• Person-months of effort • Software size

Table 2. Example Management Indicators

Metrics (or indicators) are computed from measures. They are quantifiable indices used to compare software products, processes, or projects or to predict their outcomes. With metrics, we can:

- **Monitor** requirements,
- **Predict** development resources,
- **Track** development progress, and
- **Understand** maintenance costs.

Metrics are used to compare the current state of your program with past performance or prior estimates and are derived from earlier data from within the program. They show *trends* of increasing or decreasing values, relative only to the previous value of the same metric. They also show containment or breeches of pre-established limits, such as allowable latent defects.

Metrics are also useful for determining a *"business strategy"* (how resources are being used and consumed). For example, in producing hardware, management looks at a set of metrics for scrap and rework. From a software standpoint, you will want to see the same information on how much money, time, and manpower the process consumes that does not contribute to the end product. One way a software program might consume too many resources is if errors made in the requirements phase were not discovered and corrected until the coding phase.

Management metrics are measurements that help evaluate how well the acquisition office is proceeding in accomplishing their acquisition plan or how well the contractor is proceeding in accomplishing their Software Development Plan. Trends in management metrics support forecasts of future progress, early trouble detection, and realism in plan adjustments. Software product attributes are measured to arrive at product metrics which determine user satisfaction with the delivered product or service. From the user's perspective, product attributes can be reliability, ease-of-use, timeliness, technical support, responsiveness, problem domain knowledge and understanding, and effectiveness (creative solution to the problem domain). Product attributes are measured to evaluate software quality factors, such as efficiency, integrity, reliability, survivability, usability, correctness, maintainability, verifiability, expandability, flexibility, portability, reusability, and interoperability. Process metrics are used to gauge organizations, tools, techniques, and procedures used to develop and deliver software products.

Process attributes are measured to determine the status of each phase of development (from requirements analysis to user acceptance) and of resources (dollars, people, and schedule) that impact each phase.

There are five classes of metrics generally used from a commercial perspective to measure the quantity and quality of software. During development technical and defect metrics are used. After market metrics are then collected which include user satisfaction, warranty, and reputation.

- **Technical metrics** are used to determine whether the code is well-structured, that manuals for hardware and software use are adequate, that documentation is complete, correct, and up to-date. Technical metrics also describe the external characteristics of the system's implementation.
- **Defect metrics** are used to determine that the system does not erroneously process data, does not abnormally terminate, and does not do the many other things associated with the failure of a software-intensive system.
- **End-user satisfaction** metrics are used to describe the value received from using the system.
- **Warranty metrics** reflect specific revenues and expenditures associated with correcting software defects on a case-by-case basis. These metrics are influenced

by the level of defects, willingness of users to come forth with complaints, and the willingness and ability of the software developer to accommodate the user.

- **Reputation metrics** are used to assess perceived user satisfaction with the software and may generate the most value, since it can strongly influence what software is acquired. Reputation may differ significantly from actual satisfaction:
  - Because individual users may use only a small fraction of the functions provided in any software package; and
  - Because marketing and advertising often influence buyer perceptions of software quality more than actual use.

III. SOFTWARE MEASUREMENT PROCESS

The software measurement process must be an objective, orderly method for quantifying, assessing, adjusting, and ultimately improving the development process. Data are collected based on known, or anticipated, development issues, concerns, and questions. They are then analyzed with respect to the software development process and products. The measurement process is used to assess quality, progress, and performance throughout all life cycle phases. The key components of an effective measurement process are:

- Clearly defined software development issues and the measure (data elements) needed to provide insight into those issues;
- Processing of collected data into graphical or tabular reports (indicators) to aid in issue analysis;
- Analysis of indicators to provide insight into development issues; and,
- Use of analysis results to implement process improvements and identify new issues and problems.

III.1. Typical Software Measurements and Metrics

A comprehensive list of industry metrics is available for software engineering management use, ranging from high-level effort and software size measures to detailed requirements measures and personnel information. *Quality*, not quantity, should be the guiding factor in selecting metrics. It is best to choose a small, meaningful set of metrics that have solid baselines in a similar environment. A typical set of metrics might include:

- Quality,
- Size,
- Complexity,
- Requirements,
- Effort,
- Productivity,
- Cost and schedule,
- Scrap and rework, and
- Support.

Quality

Measuring product quality is difficult for a number of reasons. One reason is the lack of a precise definition for quality. Quality can be defined as the degree of excellence that is measurable in your product. Software quality is the degree to which a system, component, or process meets:

- Specified requirements

- Customer or user needs or expectations.

Quality is in the eye of the user! For some programs, product quality might be defined as reliability [i.e., a low failure density (rate)], while on others maintainability is the requirement for a quality product. Because requirements differ among programs, quality attributes will also vary.

Size

Software size is indicative of the effort required. Software size metrics have been discussed above as SLOC and function points.

Complexity

Complexity measures focus on designs and actual code. They assume there is a direct correlation between design complexity and design errors, and code complexity and latent defects. By recognizing the properties of each that correlate to their complexity, we can identify those highrisk applications that either should be revised or subjected to additional testing.

Those software properties which correlate to how complex it is are size, interfaces among modules (usually measured as *fan-in*, the number of modules invoking a given application, or *fan-out*, the number of modules invoked by a given application), and structure (the number of paths within a module). Complexity metrics help determine the number and type of tests needed to cover the design (interfaces or calls) or coded logic (branches and statements).

There are several accepted methods for measuring complexity, most of which can be calculated by using automated tools.

Requirements

Requirements changes are a major source of software size risk. If not controlled and baselined, requirements will continue to grow, increasing cost, schedule, and fielded defects. If requirements evolve as the software evolves, it is next to impossible to develop a successful product.

An undisciplined requirements process is characterized by:

- Inadequate requirements definition,
- Late requirements clarification,
- Derived requirements changes,
- Requirements creep, and
- Requirements baselined late.

Once requirements have been defined, analyzed, and written into the System Requirements Specification (SRS), they must be tracked throughout subsequent phases of development. The design process translates user-specified (or explicit) requirements into derived (or implicit) requirements necessary for the solution to be turned into code. This multiplies requirements by a factor of sometimes hundreds.

Each implicit requirement must be fulfilled, traced back to an explicit requirement, and addressed in design and test planning.

Missing requirements may not become apparent until system integration testing, where the cost to correct this problem is exponentially high.

Effort

The relationships between duration and effort are quite complex, nonlinear functions. Many empirical studies over the years have shown that manpower in large developments builds up in a characteristic way and that it is a complex power

function of software size and duration. Many estimation models were introduced, the best known of which is Barry Boehm's COnstructive COst MOdel (COCOMO).

Productivity

Software productivity is measured in the number of lines-of-code or function delivered (i.e., SLOC that have been produced, tested, and documented) per staff month that result in an acceptable and usable system.

Boehm explains there are three basic ways to improve software development productivity.

- Reduce the cost-driver multipliers,
- Reduce the amount of code; and,
- Reduce the scalable factor that relates the number of instructions to the number of man months or dollars.

Cost and Schedule

Multi-source cost and schedule estimation is the use of multiple, independent organizations, techniques, and models to estimate cost and schedule, including analysis and iteration of the differences between estimates. Whenever possible, multiple sources should be used for estimating any unknowns, not just cost and schedule. Errors or omissions in estimates can often be identified by comparing one with another. Comparative estimates also provide a sounder set of *"should costs"* upon which to control software development. As with size estimates, assessment from alternate sources (such as program office software technical staff, prime or subcontractors, or professional consulting firms) is advisable for cost and schedule. Reassessments throughout the program life cycle improve the quality of estimates as requirements become better understood and refined. The following summarizes the resources you should consider when costing software development.

- **Human resources**. This includes the number and qualifications of the people required, as well as their functional specialties. Boehm asserts that *human resources are the most significant cost drivers on a software development effort*. Development personnel skills and experience (reflected in their productivity) have the greatest effect on cost and schedule.
- **Hardware resources**. This includes development (host) and target computers, and compilers. Hardware resources used to be major cost drivers when development personnel needed to share equipment with multiple constituencies. Now that virtually everyone has a PC or workstation on his or her desk, the issue is whether the target computer significantly differs from the development computer. For instance, if the target machine is an air or spaceborne system, the actual CPU may be technology-driven and not usable for all required development activities.
- **Software resources**. Software is also used as a tool to develop other software. Tools needed for development, test, and code generation must be considered. Your toolset might include: business systems planning tools, program management tools, support tools, analysis and design tools, programming tools, integration and test tools, prototyping and simulation tools, maintenance tools, cost/schedule estimating tools, and architectural tools.
- **Reusable resources**. Reusable assets are a valuable resource that must be considered in determining your cost requirements. This includes the assets you will develop for future reuse by other programs, as well as searching the reuse repositories for existing code that can be integrated into your development. Reusable assets will have significant impact on your program cost and schedule.

Schedule measurements track the contractor's performance towards meeting commitments, dates, and milestones. Milestone performance metrics give you a graphical portrayal (data plots and graphs) of program activities and planned delivery dates. It is essential that what constitutes progress slippage and revisions is understood and agreed upon by both the developer and the customer. Therefore, entry and exit criteria for each event or activity must be agreed upon at contract award. A caution in interpreting schedule metrics is to keep in mind that many activities occur simultaneously. Slips in one or more activities usually impact on others. Look for problems in process and *never, never sacrifice quality for schedule!*

Scrap and Rework

A major factor in both software development cost and schedule is that which is either scrapped or reworked. The costs of conformance are the normal costs of preventing defects or other conditions that may result in the scrapping or reworking of the software. The costs of nonconformance are those costs associated with redoing a task due to the introduction of an error, defect, or failure on initial execution (including costs associated with fixing failures that occur after the system is operational, i.e., scrap and rework cost).

Rework costs are very high. Defects that result in rework are one of the most significant sources of risk in terms of cost, delays, and performance.

Rework risk can be controlled by:

- Implementing procedures to identify defects as early as possible;
- Examining the root causes of defects and introducing process improvements to reduce or eliminate future defects; and
- Developing incentives that reward contractors/developers for early and comprehensive defect detection and removal.

Support

Software supportability progress can be measured by tracking certain key supportability characteristics. With these measures, both the developer and the acquirer obtain knowledge which can be focused to control supportability.

- **Memory size**. These metric tracks spare memory over time. The spare memory percentage should not go below the specification requirement.
- **Input/output**. This metric tracks the amount of spare I/O capacity as a function of time. The capacity should not go below the specification requirement.
- **Throughput**. This metric tracks the amount of throughput capacity as a function of time. The capacity should not go below specification requirements.
- **Average module size**. This metric tracks the average module size as a function of time. The module size should not exceed the specification requirement.
- **Module complexity**. This metric tracks the average complexity figure over time. The average complexity should not exceed the specification requirement.
- **Error rate**. This metric tracks the number of errors compared to number of errors corrected over time. The difference between the two is the number of errors still open over time. This metric can be used as a value for tested software reliability in the environment for which it was designed.
- **Supportability**. These metric tracks the average time required to correct a deficiency over time. The measure should either remain constant or the average time should decrease. A decreasing average time indicates supportability improvement.

- **Lines-of-code changed**. These metric tracks the average lines-of-code changed per deficiency corrected when measured over time. The number should remain constant to show the complexity is not increasing and that ease of change is not being degraded.

III.2. Collect the Measurement Data

From the definition of the specific measures, collection process requirements can be identified. These requirements are used to guide the development of the measurement data collection process.

This activity is simply the execution of the measurement data collection process.

As stated above, metrics are representations of the software and the software development process that produces them — the more mature the software development process, the more advanced the metrics process. A well-managed process, with a well-defined data collection effort embedded within it, provides better data and more reliable metrics. Accurate data collection is the basis of a good metrics process.

III.3. Analyze the Measurement Data to Derive Indicators

Indicators are derived from the analysis performed on the measurement data. The quality of the indicator is tied to the rigor of the analysis process.

Both objective and subjective measures are important to consider when assessing the current state of your program. Objective data consists of actual item counts (e.g., staff hours, SLOC, function points, components, test items, units coded, changes, or errors) that can be independently verified. Objective data are collected through a formal data collection process. Subjective data are based on an individual's (or group's) feeling or understanding of a certain characteristic or condition (e.g., level of problem difficulty, degree of new technology involved, stability of requirements). Objective and subjective data together serve as a system of checks and balances throughout the life cycle.

Analysis of the collected data must determine which issues are being addressed, and if new issues have emerged. Before making decisions and taking action from the data, you must thoroughly understand what the metrics mean.

Cost data usually reflect measures of effort. Process data usually reflect information about the programs (such as methodology, tools, and techniques used) and information about personnel experience and training. Product data include size, change, and defect information and the results of statistical analyses of delivered code.

III.4. Manage the Measurement Data and Indicators

The measurement data and the indicators must be properly managed according to the requirements identified in the measurement plan.

III.5. Report the Indicators

Once the indicators are derived, they are made available to all those affected by the indicators or by the decisions made because of the indicators.

III.6. Evaluation

The value of any measurement process is in direct proportion to the value the indicators have to the users of the indicators.

III.7. Review Usability of Indicators

Initially, the selection of indicators, analysis methods, and specific measurement data may be a 'best guess' whether or not they meet the information needs specified. Over time, through a review of the usefulness of the indicators, the selection can be refined such that there is a high correlation between the indicators selected and the information needs.

III.8. Begin Measurement Activities Early

Measurement, as a practice, must begin at the project level. Other activities such as project planning, project monitoring, etc. rely on the information gathered by the measurement process.

As the organization begins to focus on process standardization and improvement, the measurement program grows. Additional "information needs" are identified and fed to the measurement process. More mature processes such as quantitative process management, process innovation deployment rely on indicators to determine effectiveness, efficiency, and productivity, etc.

IV. CAUTIONS ABOUT METRICS

Software measures are valuable for gaining insight into software development; however, they are not a solution to issues in and of themselves. To implement a metrics program effectively, you must be aware of limitations and constraints.

- **Metrics must be used as indicators, not as absolutes**. Metrics should be used to prompt additional questions and assessments not necessarily apparent from the measures themselves. For instance, you may want to know why the staff level is below what was planned. Perhaps there is some underlying problem, or perhaps original manpower estimates need adjusting. Metrics cannot be applied in a vacuum, but must be combined with program knowledge to reach correct conclusions.
- **Metrics are only as good as the data that support them**. Input data must be timely, consistent, and accurate. A deficiency in any of these areas can skew the metrics derived from the data and lead to false conclusions.
- **Metrics must be understood to be of value**. This means understanding what the low-level measurement data represent and how they relate to the overall development process. You must look beyond the data and measurement process to understand what is really going on. For example, if there is a sharp decrease in defect detection and an increase in defect resolution and close out, you might conclude that the number of inserted defects is decreasing. However, in a resource-constrained environment, the defect discovery rate may have dropped because engineering resources were temporarily moved from defect detection (e.g., testing) to defect correction.
- **Metrics should not be used to judge your contractor (or individual) performance**. Measurement requires a team effort. While it is necessary to impose contractual provisions to implement software measurement, it is important not to make metrics a controversial issue between you and your contractor. *Support of the measurement process will be jeopardized if you "shoot-the-messenger."* Measurements should be used to identify problem areas and for improving the process and product. While metrics may deal with personnel and

organizational data, these data must be used for constructive, process-oriented decision-making, rather than for placing blame on individuals or teams.

- **Metrics cannot identify, explain, or predict everything**. Metrics must be used in concert with sound, hands-on management practice. They are only valuable if used to augment and enhance intimate process knowledge and understanding.
- **Analysis of metrics should NOT be performed exclusively by the contractor**. Ideally, the contractor you select will already have a metrics process in place. As mentioned above, you should implement your own independent metrics analysis process because:
    - Metrics analysis is an iterative process reflecting issues and problems that vary throughout the development cycle;
    - The natural tendency of contractors is to present the program in the best light; therefore, independent government analysis of the data is necessary to avoid misrepresentation; and
    - Metrics analysis must be issue-driven and the government and contractor have inherently different issue perspectives.
- **Direct comparisons of programs should be avoided**. No two programs are alike; therefore, any historical data must be tailored to your program specifics to derive meaningful projections. *[Conversely, do not tailor your data to match historical data.]* However, metrics from other programs should be used as a means to establish *normative values* for analysis purposes.
- **A single metric should not be used**. No single metric can provide the insight needed to address all program issues. Most issues require multiple data items to be sufficiently characterized. Because metrics are interrelated, you must correlate trends across multiple metrics.

REFERENCES

- Boehm, Barry W., *Software Engineering Economics*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981
- Boehm, Barry W., as quoted by Ware Myers, *Software Pivotal to Strategic Defense,* IEEE Computer, January 1989
- Campbell, Luke and Brian Koster, *Software Metrics: Adding Engineering Rigor to a Currently Ephemeral Process*, briefing presented to the McGrummwell F/A-24 CDR course, 1995
- DeMarco, Tom, *Controlling Software Projects*, Yourdon Press, New York, 1986
- *IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.12-1990*, Institute of Electrical and Electronic Engineers, Inc., New York, NY, December 10, 1990
- Marciniak, John J. and Donald J. Reifer, *Software Acquisition Management: Managing the Acquisition of Custom Software Systems*, John Wiley & Sons, Inc., New York, 1990
- Pressman, Roger S., *Software Engineering: A Practitioner's Approach*, Third Edition, McGraw-Hill, Inc., New York, 1992
- Rozum, James A., *Software Measurement Concepts for Acquisition Program Managers*, Technical Report CMU/SEI-92-TR-11/ESD-TR-92-11, Carnegie-Mellon University, Software Engineering Institute, Pittsburgh, Pennsylvania, June 1992.