Natasa Aleksic[1)]
Milan Eric[2)]

Faculty of Engineering, University of Kragujevac, Serbia
aleksicnatasa0@gmail.com, ericm@kg.ac.rs

CUSTOMER SATISFACTION QUALITY MANAGEMENT IN HIGHER EDUCATION

Abstract: *Starting with the rapid changes in information technologies and the growing contribution of modern science research methodology, a natural need to high school vocational study analyzes the requirements, please follow the scientific and technical achievements and introducing new technologies that are acceptable to users highly educational services. Through a system of quality management is improved customer satisfaction and all processes in high vocational school kept under control.*
Keywords: *quality management, information security, ISMS*

1. INTRODUCTION

By knowing the information he becomes more successful in their work and creative creation, prevents accidents, bad decisions and solutions, neutralize errors, reduces the impact of contingencies. Of course, how the information has some value it becomes the target of theft, abuse, discredit. No matter in what form the information stored must be adequately protected. To ensure adequate protection of information, all users must be familiar with the concept of the protection measures that are required.

Opening information resources institutions of higher education to the outside world has its negative side. Information and IT resources (hardware and software) are exposed to numerous security threats such as computer fraud, industrial espionage, sabotage hacking, viruses, etc. Survival of high school vocational study is directly related to its ability to protect its information value. That concept of protection or security clearance information to the fore.

At the present time to establish a secure information system has been identified as a need to develop a number of standards that include best practices and recommendations on the management of information security. Safety information in one system is a reality and needs. Building unmanaged security system is a necessity in the business world, but also increasingly in other higher education institutions.

In the process of developing the strategy for the development of higher education is the idea that high school vocational studies functionally integrate in order to achieve quality education and scientific work. For this purpose enables the teaching staff, strengthen supervision of professional services, conducted training of all employees.

Examples of the recent past are indications that high school vocational studies must promote their business, not only in the field of quality management, but also in the field of their own information, as well as in the field of better security system. With regard to many high vocational school and universities introduced IT security (security information).

In addition, to improve the security of information must be provided better

security systems, which are involved in joint problem solving.

Case studies should also include research in the field of reducing the risk of damage or loss of information, reduce costs, compliance with applicable laws and regulations, competitive advantage, greater confidence of customers, employees, associates, institutions and all stakeholders in the knowledge that their data is safe also aware of the responsibility for the security of information by all and at all levels of higher education institutions.

Some of these problems are:

- Direct financial losses due to fraud
- Loss of valuable and confidential information
- Unauthorized use of resources
- Loss of business reputation and customer confidence
- Increased costs caused by uncertain business conditions

2. ANALYZES INFORMATION SYSTEM

Analyzes information system is performed according to agreed principles and rights of the ISO 27001 standard. The analysis itself is necessary in order to facilitate detection of flaws and vulnerabilities, ie. determining risk. Certain assumptions, ie. documents include, but are part of a plan to establish the ISMS are met. This primarily refers to the written record management support and creating security structures of higher education institutions. [1]

In an institution such as a school it is difficult to define and create a security structure where the number of people involved in the security process is very small.

2.1 The organizational structure of the authority and responsibilities of highly - technical school of professional studies

Institutions of higher education is set to work processes at a high - Technical School with the intention that, within the defined activities, achieve set goals. In the institution of higher education director appointed by the members of management with executive responsibility of the perpetrators assigned tasks whose execution was necessary to achieve the work process, in accordance with the Act on Higher Education.

The very structure of institutions of higher education is defined within the statute of school, are shown in Figure 1.

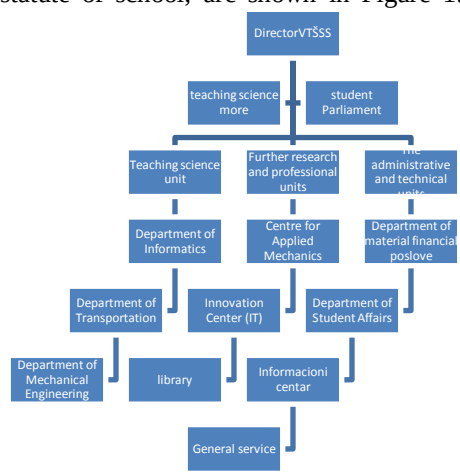

Figure 1 - Scheme of inner structure VTŠSS which assures quality

2.2 Asset Management

The aim is to achieve and maintain asset protection institutions. Develops the inventory of assets within the scope of the ISMS, and estimated the value of the same. One of the most important tasks of establishing ISMS is a list of assets. VTŠSS so far had made the list.

As this is a necessary precondition for any talks on security, and consequently spent the most time in this job.

The quality of the classification of assets as well as determining the relationship between the individual resources depends on the determination of risk information system as a central part of

the system.

Specifies the responsibility for maintaining the property over planned controls. Detail to determine the security classification of assets (Table 1) and confer access rights thereto.

Irrespective of the nature of information resources (information values) (Table 1) may have one or more of the following effects are:[2]

- Identify the level at institutions of higher education as an entity that has value
- You can easily be replaced without the expenditure of resources, such as money, skills of employees, time, etc.
- Make the identity of higher education institutions without whom the business college of professional studies may be compromised

Table 1 - Classification of assets

Category	Description
Information	Information is the most important type of resources
Processes and Services	The processes and services include business process, application activities, operational services and other services that allow information processing
Software support	The software includes application programs, system programs, helper applications ...
Hardware	Includes computers, communications equipment, media, technical equipment and the like
People	This category includes people, clients, service users and others who have any role in storing and processing information
Location	This category includes'm accommodate all the above categories, especially if the institution is composed of several buildings in different locations

3. RISK ASSESSMENT METHODOLOGY

The process of risk management is an increasingly important in protecting information assets and business processes because it is the basis for building a secure and reliable IT infrastructure. To allow better and more efficient decision-making related to the improvement and enhancement of safety, it is necessary to identify the critical parts of the structure, and determine the associated security risks. Without high-quality analysis and risk assessment information structure, it is very difficult to develop and implement safe composition.

The Technical College of Vocational Studies realized that their data is insecure, vulnerable, and are for that reason began to deal with more issues.

New vulnerabilities are discovered every day and published in the security community, refentnim various mailing lists and forums that deal with information security. There are several methods for detecting vulnerabilities with which achieves transparency in service delivery, and management of high-level, as well as a mechanism for clearly visible and tangible evidence of cost reduction through better risk management, and reducing the importance of causes of errors in an institution of higher education.

This method of risk assessment uses three parameters: the value of resources, threats and vulnerabilities. Each of these parameters is observed in relation to the possible consequences, while threats are considered in relation to the corresponding vulnerability.

All parameters are quantified arbitrarily. Information about property values determine the owners of these

resources. [3]

- AV - the value of resources, assets
- V – vulnerability
- T – threat

To determine the value of resources used numerical values ranging from 0 (low) to 4 (very high), while for the quantification of vulnerability and threats using a scale from 0 (low) to 2 (high level). [4]

Risk levels are determined by the sum of the values of parameters, that is

R = AV + V + T

The minimum and maximum value of the estimated risks are:

Armin Armin = Vmin + + Tmin = 0

Rmax = AVmax Vmax + + Tmax = 8

Determining the risk of a resource is determined at the end of the predefined table of values (Table 2)

Property value is determined in relation to all three attributes so. Three (confidentiality, integrity, availability - PID (Eng. CIA)) (Tables 3, 4 and 5)

Table 2 - Dedicated risk values

Levels threats		**Low**			**Medium**			**Large**		
levels of vulnerability		N	S	V	N	S	V	N	S	V
value of assets	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Each risk is high, it is necessary to reduce in the short period of time.

For medium risk reaction time increases, but is still important to react quickly depending on the valuation of property.

At the end of the low risk it is important that he does not ignore the process of reducing risk.

Table 3 - Interpretation Risk

Value	Risk	operating time
0 – 2	Low	< 6 months
3 – 5	Medium	< 2 months
6 -8	Large	< 2 daay

3.1 Data Classification

a) Confidentiality

Table 4 - Determination value in relation to confidentiality

Value	Degree	Description
0 or small	Public	Without restrictions
1 or medium	confidential	All employees and teachers have access to with the approval of the Director
2 or large	secretly	Limited access to the Director and Secretariat

b) Integrity

Table 5 - Determination value of the property in relation to the integrity

Value	Degree	Description
2 or large	High	Strategic data may not have the wrong values, is to detect and repair
1 or medium	Medium	Important for the business process, but no significant impact on decisions or other IT systems
0 or small	Low	It can not tolerate wrong information, it will be repaired at a future action or the user will perceive how I error

Results of the analysis will be particularly pointed out in the following paragraphs, where will explicitly specify all the threats, vulnerability and the observed value of the property.

c) Availability

Table 6 - Determination of value in relation to the availability

Description	Degree		
	Low	Medium	High
Working day	Mon – Fri	Mon –Fri	7 day
Time of resources	7:30-16:00	7:30-16:00	24 hours
Time delays in failure	1 day/ week	2 hors/ week	12 min / week
Maximum deadlock by faulty	1 week	1 day	1 hours
Expected availability	80%	95%	99.9%

As part of the risk analysis, there are vulnerabilities and threats resulting in a penetration test system.

3.2 Penetration test system VTŠSS

Checking the security of the information system of examining vulnerability and penetration testing (penetration test, eng. Penetration) is an essential process by which institutions of higher education and identify threats to information assets, the purpose of calculating the level of risk and selection of appropriate protective measures.

Testing vulnerability penetration test in the VTS is made free or trial tools. The test is performed remotely, to check a Linux server, but also in space VTŠSS (Eng. on-site) for checking the "internal network".

The tools that were used in the test:

- Nessus Security scanner 3
- GFI LANguard Network Security Scanner 8.0
- SANS Qualys top 20 scanner
- Metasploit 3 i Nmap
- Ophcrack

The test results of the system are inserted into the analysis system, the specific threat was amended procedure for determining risk. Reports obtained from individual applications for security reasons will not be attached to this work, but will be included in the GLPI database system.

Testing of the system is also possible and by independent analysts. This method of testing will be done only when implementing security solutions stem from current opinion.

In the following presentation, the table is described and represented only part of the analysis results.

3.2.1 Analysis results

a) Inventory

Table 7 - List of assets

Category	Name of resource	Owner	C	I	A	Max. (C,I,A)	Value of resources
Information	Financial Data	Account	V	V	M	V	4
Information	Own documents	Director	V	V	V	V	4
Information	Data on students	Educator	V	V	S	V	4
Processes and services	DNS www.vts.edu.rs	Admin.	V	V	V	V	4
Processes and services	WEB www.vts.edu.rs	Admin.	V	V	V	V	4
Processes and services	E – pošta (webmail)	Admin.	V	V	V	V	4

Hardware	Thin Clients	Prof. Infor.	M	M	M	M	1
Hardware	Wireless AP	Admin.	V	V	V	V	4
Peaple	IT admin.	Director	V	V	S	V	4
Location	Space Informatics	Professor of Computer Science	M	V	S	V	3

b) Risk assessment

In the process of risk assessment of individual services within the information system must be connected to the respective computer that is running. In this way, combine resources, and getting the best knowledge of vulnerabilities and threats to those assets.

This information system will be grouped the following resources which will be considered as a whole:

- Servers with OS Linux Debian 4.0 (DNS, web, forums, web mail;
- Server sa Windows server 2003 (Active Directory, DHCP, File sharing, uslugama, interna domena nkg.local) ;
- Desktop computers with Windows XP Professional;
- E-classroom ie classroom (Windows XP Embedded thin clients + windows server)

This system is abundant lack of documentation, for this reason is not in the risk evaluation determined this category of vulnerability, unless it is necessary to specify the particular property that vulnerability.

One of the basic ideas of ISMS is to determine which documents should be seated. [5]

Assets - categories of information

Table 8 - Value Risk category information

Asset	Vulnerability	estimation of the vulnerability	a threat	the threats estimation of thei	Risk
Financial Data	Data archiving	M	data Loss	S	5
Own documents Director	Data archiving	S	data Loss	S	6
Data on students Educator	Data archiving	M	data Loss	S	5
E - mail for all users	Data archiving	V	data Loss	S	7

a) Assets – software

Table 9 - Value-risk categories of software

Asset	Vulnerability	estimation of the vulnerability	a threat	the threats estimation of thei	Risk
Windows Server_1	Lack of security updates	V	The exploitation of known vulnerabilities	V	8
	Problems with user computers	V	Unauthorized access to information	V	8
	data archiving	S	data Loss	S	6
	data	M	data	S	5

	archiving		Loss		
	data archiving	V	data Loss	V	8
MS Office 2003 + ostale kancelar. Aplikacije	Lack of security updates	S	The exploitation of known vulnerabilities	S	4
Windows XP Professional	Lack of security updates	S	The exploitation of known vulnerabilities	V	6
	Running applications with portable memory	V	Unauthorized access to data	N	2
Windows XP Embedded	user authentication	N	Unauthorized access to data	N	2
MySQL	data archiving	S	data Loss	S	4

b) Assets – Hardware

Table 10 - The value of the risk categories of hardware

Asset	Vulnerability	n of the vulnerabil ity	a threat	threats estimatio n of thei	Risk
Thin clients	Defective irregular maintenance	M	degradation of service	M	2
Linux server_1 Wireless AP	Defective irregular maintenance	V	denial of Service	V	8
	Defective irregular maintenance	V	denial of Service	V	8
Windows server_1	Defective irregular maintenance	V	denial of Service	V	8
Windows server_2	Defective irregular maintenance	S	denial of Service	S	6
Desktop computers	Defective irregular maintenance	M	degradation of Service	M	2
Media warehous. Floppy disks, optical, USB memory	damage to the media	S	unavailable information	S	6
DSL modem	Defective, irregular maintenance	S	Denial of Service	M	2
	user authentication	S	Denial of Service	M	2
UPS	Stamina battery	M	Denial of Service	S	3

c) Assets - Others (people, locations)

Table 11 - Value of risk category Others

Asset	Vulnerability	estimation of the vulnerability	a threat	the threats estimation of thei	Risk
IT administrator	There are no written procedures / standards	V	unauthorized activity	V	8
	Dissatisfaction in the transactional	M	Revealing confidential information	V	8
accountant	Needucir. workers	M	mproper use org.resursa	V	5
	Needucir. workers	M	unauthorized activities	V	5
students	Needucir. workers	M	Denial of Service	V	3
professors	Needucir. workers	M	unauthorized activities	V	4
educator	Needucir. workers	M	Revealing confidential information	V	5

3.2.2 Reducing the risk evaluation

From the results of risk assessment, tables 8, 9, 10, and 11, it is evident that the key resources servers. Threats are mostly technical in nature and they are: nedokumentiranost, system, data warehousing, security updates and more. However, as the greatest flaw of the system I noted the absence of the DMZ. Most risks will disappear establishing the DMZ and system upgrades.

The risk that will remain will eventually decline, but will always be present. Primarily refers to the human factor. In reducing that risk a major role to play primarily education professor, and later students.

I pointed out the student as a category of users who would usually push the boundaries of safety. Quality composition hiring professors can reduce the risk of this group of users, perhaps even eliminated.

Creation of full system even though it looks like a big problem, in fact it's not so bad. Most of the actions related to safety is present, but not procedurally explained. The problem is in the execution of other actions that have not been explicitly specified. Work habits administrator, and it can be said of all the people, that if something is not specified, usually in paper form as a contract, it is not executed. Because of these facts it is necessary to identify and order the execution of such work action.

It is therefore necessary administrative support, in this case, the school principal as an organ of coercion.

4. CONCLUSIONS

Modern business practice shows that the problem of information security is not an exclusive problem of information technology, but it is more "business" problem which has to deal with the highest level of management institutions of higher education. At its core is a problem of management (management) risks. Standard ISO / IEC 27001:2005 gives one a harmonized approach to managing the risks to which they are exposed to information value in institutions of higher education through the development, implementation and maintenance management system for information security (Information Security

Management System - ISMS).

REFERENCES:

[1] Kenning, M., "Security management standard -ISO 17799/BS 7799" BT Technology Journal, 19 (2001) 132-136.
[2] Humphreys, T., Plate, A., "An International Common Language for Information Security" *ISMS Journal*, 6 (2-3) (2006).
[3] Vermeulen, C., Van Solms, R., "The infomation security management toolbox - taking the pain out of security management" *Information Management & Computer Security*, 10 (3) (2002) 119-125.
[4] Broderick, S., "*ISMS, security standards and security regulations*" *Information Security Technical Report IT* (2006) 26-31.
[5] Solms, R., "Information security management: why standards are important" *Information Management & Computer Security* 7 (1) (1999) 50-57.