Vladimir Šimović
Matija Varga
Predrag Oreški

Case Study: an Information System Management Model

Article Info:

Management Information Systems,
Vol. 7 (2012), No. 1,
pp. 013-024

Received 28 December 2011
Accepted 24 January 2012

UDC 007:005]:004

Summary

This article presents the purchase management information system, finance management information system and security information system, their interdependence and tight correlation. Furthermore, we state the goals of the purchase management information system that must be achieved in any organisation, as the purchase (sub)process is carried out in every organisation. P-K matrix gives a detailed presentation of a public organisation, and data classes and sub-processes within the observed organisation. Other companies involved in similar activities can perform their processes in accordance with the presented business technology matrix. The business technology matrix was used for designing a data flow process diagram comprising data flow, warehouses, processes and the external entity which can also be used in such companies. The article also deals with the duration of the sub-processes. The duration of sub-processes must be reduced as much as possible in order to achieve the planned result at the process output point. A hypothesis was set in the article, for the period from the beginning of 2009 until the end of 2010. We observed whether the total cost-effectives coefficient in the company would fall under the threshold value of 1. The article has proven that, based on the sample (profit-and-loss account), there is no reason to discard the H0 hypothesis, as the company's total cost-effectiveness coefficient did not fall below the permitted value of 1 for two years. The third section of the article presents the possible threat to organisations' information systems, and describes methods of protecting electronic information in processes, and recovering electronic databases in finance management information systems.

Keywords

purchase management information system, finance management and security information system, P-K matrix, data flow diagram, financial report analysis, cost-effectiveness indicators

1. Introduction

Along with support in decision-making, the managerial information system serves as support to managers when making decisions. Decisions are frequently made in the purchase information system, based on information from the finance information system. More often than not, relevant information required in the purchase process are gathered from financial reports. This article presents cost effectiveness over a period of five years in the financial report analysis process, to that the hypothesis was set at the outset of the long-term research, in 2008. Overal cost-effective coefficients for the period from 2005 until the end of 2008 were known, so that they were not taken into consideration when setting the hypothesis. The hypothesis was set for the period from the beginning of 2009 until December 31, 2010. H_0 denotes null hypothesis, whereas H_1 is the mark for the alternative hypothesis. Hypothesis H_0 refers to a situation when the cost-effectiveness coefficient of the total business operation over the observed two years does not amount less than 1, when we take into account the data from financial reports of the observed company, i.e. profit-and-loss account. H_1 is the mark for the alternative hypothesis when the total cost-effectiveness coefficient is under the threshold value of 1. The article has proved that, based on the sample (profit-and-loss account) There is no reason to discard hypothesis H_0, i.e. the total cost-effectiveness coefficient has not fallen below the tolerated threshold of 1.

All the relevant information used by managers for making key decision ougth to be protected, whether they are in digital or analog form.

1.1. Aims and Tasks

The aim of this article is to describe the manner of functioning of the information systems for managing purchases, finance and security in an organisation, and their interconnectedness. These systems are essential for efficient functioning of any organisation type, regardless of property type. The basic task of the purchase management information system is to obtain all the information required for acquiring resources and other capital goods in organisations following appropriate criteria. Just-in-time (JIT) information enables

generating profit within purchase sub-processes. The additional tasks of the acquisition process include cost-cutting when purchasing resources and capital goods, thus enabling efficient operation of the entire system. The article demonstrated possible threats to the organisation's information systems, ways of protecting the information and retrieval of electronic data in the finance management information system. Within the finance management information system, the article will demonstrate a decision making support system, and indicators for measuring the progress flow in the information management information system. These three information system were taken into consideration due to the fact that are highly significant for overall management and administration, and because the purchase management is of key importance for seamless process flow in organisations. The information system is essential for recording events and changes in business, and analysing financial reports. The security management information system takes care of he protection of relevant and reliable information, and protection of electronic information of importance for the organisation.

1.2. Employed Research Methods

The research methods employed here inlude: case study, modelling (data flow diagram and business technology matrix), interview, measurement (determining the exact time), statistical methods (indexes), observation, perception, analysis (content analysis, business system analysis and other indicator system), which will be used for determining business objects, processes, events, information, documents and information system protection measures.

2. Purchase Management Information System and its Significance

It is a well-known fact that an information system is a data image of processes from objective reality. The aim of any information system is to provide the system with all necessary and relevant information for seamless execution of processes and system administration. Purchase management information system is a complicated system enabling communication of the company with its buyers and suppliers, keeping track of capital goods flow, all condition for monitoring business relationships, preparing and transferring data into the finance management information system, more precisely, into process accountancy. (Panian & Ćurko, 2010, p. 93) One cannot dispute the thesis that the purchase management system is the most important. It is used for gathering information required for seamless performance of all processes in organisations.

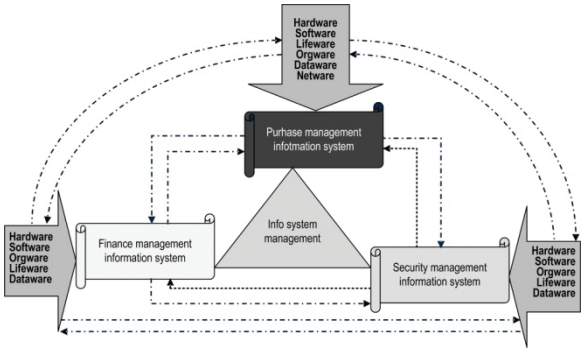


Figure 1 Connections between information systems and their parts
(Varga et al., 2007 based on condsiderations on connections between the presented information systems)

The purchase process and its sub-processes are used for purchasing or commissioning information, commodities, other capital goods, services and labour. One cannot dispute Vilim Ferišak's (2006) thesis that profit is generated in purchase. Purchasing better capital goods at prices lower than thear real value generates profit, and cuts purchase costs.

This is another piece of evidence that the purchase and finance management systems are closely connected (Figure 1). Finance management information system is also very important, as it records all business events occurring in the organisation, and takes care of the availability of funds. Security management information system cannot function without finance management information system out of which it is financed, nor can the information management system function without security management information system which protects it constantly. Figure 1 shows the interconnectedness of the above mentioned information systems and parts of the segments of information system (program segment, hardware) segment, organisation segment, human resource segment, network and data segments required for seamless operation of business processes.

2.1. Purchase Management Information System Decomposition

Purchase management information system decomposition is segmenting the system to information subsystems according to a defined order and in an appropriate manner, observing the

decomposition rule, stating that each parent must have a minimum of two offsprings..

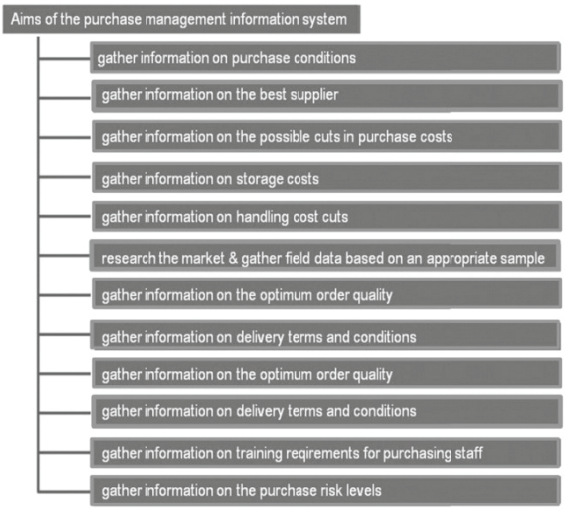


Figure 2 Decomposed aims of the purchase management information syste,
(The author's own design)

Firgure 2 illustrated decomposing the goals of the purchase management information system. The goals presented here conmprise their own sub-goals, which is obvious from the graphic models: gather information on purchase conditions; gather information on the best suplier; gather information on the possible cuts in purchase costs; gather information on storage costs; gather information on handling cost cuts; to research the market and gather field data based on an appropriate sample; gather information on the optimum order quality; gather information on delivery terms and conditions; to gather information on training requirements for purchasing staff; and gather information on the purchase risk levels.

2.2. Purchase Strategy

Purchase stategy forms a plan set in such a way that it will enable the organisation to accomplish its set goals. Purchase is an executive process consisting of numerous activities. The purchase strategy should be incorporated in the organisation's overall business strategy. Purchasing can be regarded as an organisation's subsystem, and its activities can make an impact on cost cutting and performance improvent. For the purchase prosess to function well, it is necessary to:

1. establish good relationships with business partners products are purchased from,
2. avoid dependence on a single seller,
3. upskill the purchase department staff: and motivate the staff.

The purchasing process begins from establishing the need to purchase capital goods.

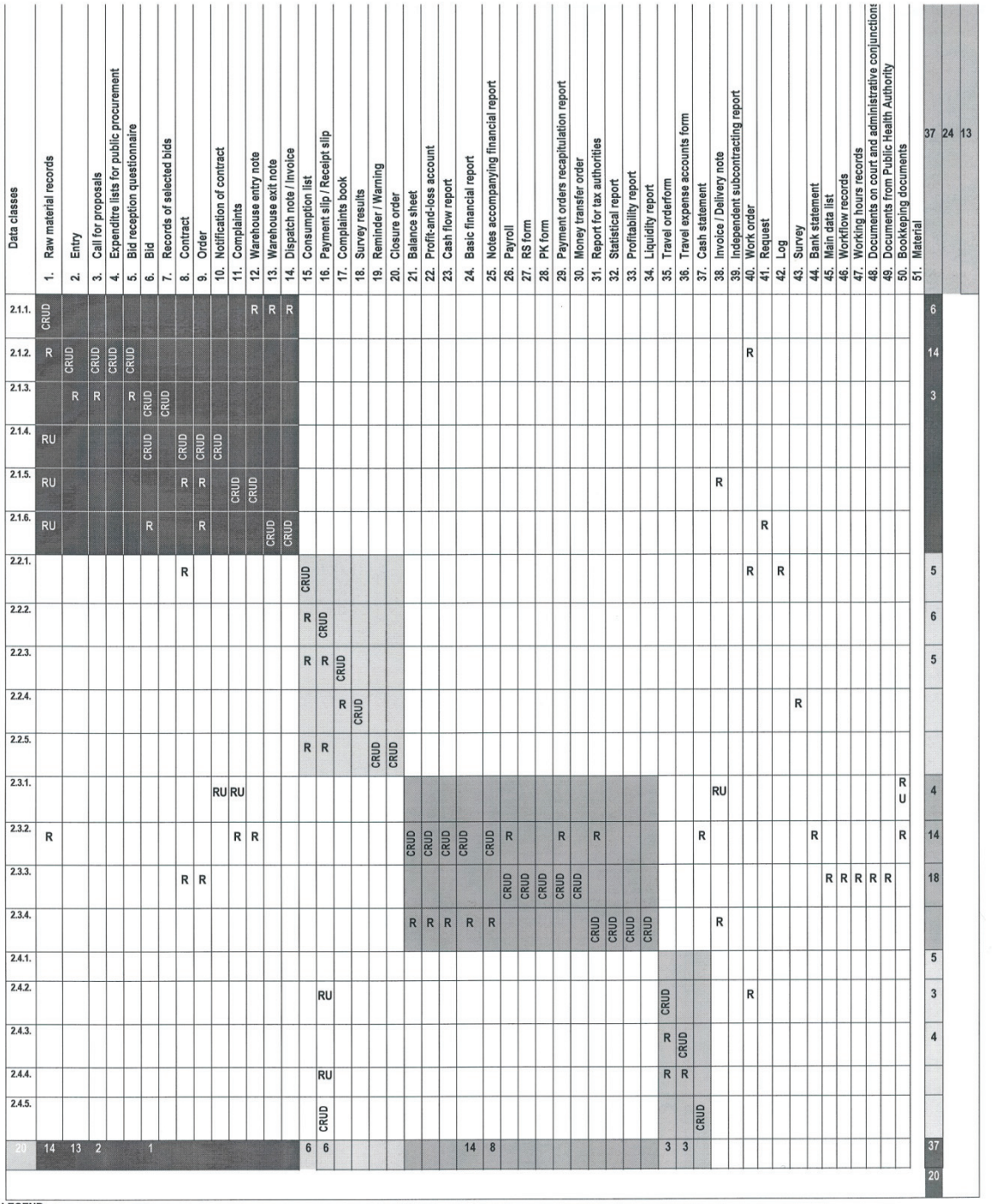
2.3. Purpose and Tasks of Purchase Management Information System

The purpose of the purchase management system is to achieve the set goals related to supplying the organisation it belongs to with all capital goods, services, energy and labour. In this they must make sure to obtain a sufficient amount of capital goods, at the most reasonable prices possible, with on-time.in-full- right-place delivery, from reliable sources, i.e. suppliers who fulfill their abilities on time and conscientiously, and provide appropriate pre-sale and aftersale service. In the case of public procurement, it is necesary to pay attention to the suppliers business abilties, which is proven through financial reports and references. The purpose of the purchasing process is to connect and harmonise the organisation's requirements for capital goods, services, labour and energy on the one hand, and the interests of the suppliers of those commodieties on the other.

2.3.1. Internal and External Document Flow in the Information, Purchase and Information Systems

The business technology matrix is a strictly defined 2D[1] mathematical strucutre, subject to formal mathematical operations such as verifying the consistency of business technology or system optimisation, and describes reslationships between various factors. (Brumec, 2007) The matrix is so structured that there is no process solely generating data classes, without using any of them. The P-K matrix is the mathematical presentation of the number of processes, sub-processes, activities and data classes. A process is a set of activities flowing in a given order. A data class is a logically shaped and connedted data set, related to a given phenomenon or entity. The business technology matrix for the supply management was partially used for creating the data flow diagram. P-k matris is more appropriate for presenting large information systems, due to clearer representation of relationships, and determining which process or sub-process creates, reads, updates and deletes strictly determined data classes.

[1] 2D denotes two demensions: (1) data classes and (2) number and names of processes.



LEGEND:

2.1.1. Establishing current inventories PPN1; 2.1.2. Announcing public call for proposal and sending enquiries PPN2; 2.1.3. Processing bids PPN3; 2.1.4. Procurement of materials and energy (goods, labour and services) PPN5; 2.1.5. Materials and energy reception PPN5; 2.1.6. Material allocation and invoicing PPN6; 2.2.1. Consumption upload PPP7; 2.2.2. Consumed gas price calculation PPP8; 2.2.3. Consumption calculation control PPP9; 2.2.4. Consumer satisfaction monitoring PPP10; 2.2.3. Recording debtors PPP11; 2.3.1. Claims settlement PPR12; 2.3.2. Ledger records PPR13; 2.3.3. Payroll calculation PPR14; 2.3.4. Compiling statistical reports and cash report analysis PPR15; 2.4.1. Payment PPB16; 2.4.2. Issuing travel orders PPB18; 2.4.3. Travel expenses report PPB19; 2.4.4. Remuneration PPB19; 2.4.5. Compiling cash statements PPB20

Figure 3 The P-K matrix
(The author's design, based on the business logic of the observed company, and established 20 sub-processes and 50 data classes with analytical data processing tools.)

Figure 3 shows a detail picture of the information system of a public organisation, divided into parts or subsystems, and its functioning. The business technology matrix offers data on the purchase management information system, and all documents required to the purchase department for seamless process flow. Figure 3 shows determined processes and data classes in accordance of phases of public procurement of

goods, labour and labour for the purchase management information system, and other information systems tightly connected to it, and collaborating on task performance. As purchase management information system is tightly connected with other information systems within the organisation, Figure 3 shows a more complex business technology matrix. A business technology matrix shows which documents, as data carriers, are required by the purchase management information system so that the suppliers can assure purchasing organisation's management that they can achiever the set goals and perform the work independently. When taking over the materials and capital goods within the purchase process, it is necessary to establish the state of the supplied product and control its condition. Several employees will participate in the takeover subprocess, as the takeover of a certain commodity requires strict controls.

The business technology matrix was analysed with an analytical data processing tool. The tools facilitated determining how many suprocesses the purchase and finance management information systems contain. The purchase management information system was found to have 6 subprocesses. A simpler combination of functions used in this analytical data processing task for analysing the business technology matrix looks as follows:

=SUM(SUM(COUNTIF(B14:V17;"R");COUNTIF(AM14:BC17;"R"));(SUM(COUNTIF(B14:V17;"RUD");COUNTIF(AM14:BC17;"RUD");(SUM(COUNTIF(B14:V17;"RU");COUNTIF(AM14:BC17;"RU")))))).

The marks in this business technology matrix are: C(retaing), R (eading), U(pdating), D(eleting) or their combination. The advantages of the business technology matrix for the representation of the information system model, or processes and data classes are: matrix (Figure 3), giving a clear and systematic overview of all data processes and classes within the observed information system, unlike the observed information system, unlike the data flow diagrams (Figure 4), which cannot be comprehensible for representing large and compels information systems. A matrix shows how many times an individual process creates, reads, deletes and updates a given data class. Based on the business technology matrix, we can conclude which documents can be created as a result of individual processes. A business technology matrix gives a clear representation of the number of processes, subprocesses, activities and data classes, and the representation of how many times a given data class is created, read, deleted and updated, but does not show the length of individual processes subprocesses and activities, which was the reason for showing in this article the time required to perform the process, unlike the previously published articles.

Table 1 shows the duration of individual subprocesses in hh:mm:ss format. Duration of individual subprocesses could not be established, so they were marked "X", Measuring the duration and progress of subprocesses in purchase, finance and security system management is significantly different than in the production information system.

Figure 4 shows a data flow diagram comprising flows, data flows, subprocesses and external entities (sources or destinations). The data flow diagram was compiled based ont he business technology matrix. Apart from the finance and purchase information system, it also shows other information systems so as to point out the interconnectedness and information exchange

Table 1 Duration of individual processes and subprocesses

Sub-processes	2.1.1. Establishing current inventories PPN_1	2.1.2. Announcing public call for proposal and sending enquiries PPN_2	2.1.3. Processing bids PPN_3	2.1.4. Procurement of materials and energy (goods, labour and services) PPN_4	2.1.5. Materials and energy reception PPN_5	2.1.6. Material allocation and invoicing PPN_6	2.2.1. Consumption upload PPP_7	2.2.2. Consumed gas price calculation PPP_8	2.2.3. Consumption calculation control PPP_9	2.2.4. Consumer satisfaction monitoring PPP_{10}	2.2.3. Recording debtors PPP_{11}	2.3.1. Claims settlement PPR_{12}	2.3.2. Ledger records PPR_{13}	2.3.3. Payroll calculation PPR_{14}	2.3.4. Compiling statistical reports and cash report analysis PPR_{15}	2.4.1. Payment PPB_{16}	2.4.2. Issuing travel orders PPB_{18}	2.4.3. Travel expenses report PPB_{19}	2.4.4. Remuneration PPB_{19}	2.4.5. Compiling cash statements PPB_{20}
Average sub-process duration time (determined based on data received from finance and commercial director	0:02:00	0:50:00	0:60:00	x	0:30:00	0:30:00	0:04:00 per meter	1:20:00 per reader on average	x	0:10:00	0:02:00	0:01:00	x	0:06:00	x	0:01:00	0:02:00	0:20:00	0:01:00	0:05:00

(The author's own design, based on information received from financial and commercial director, and calculated average)

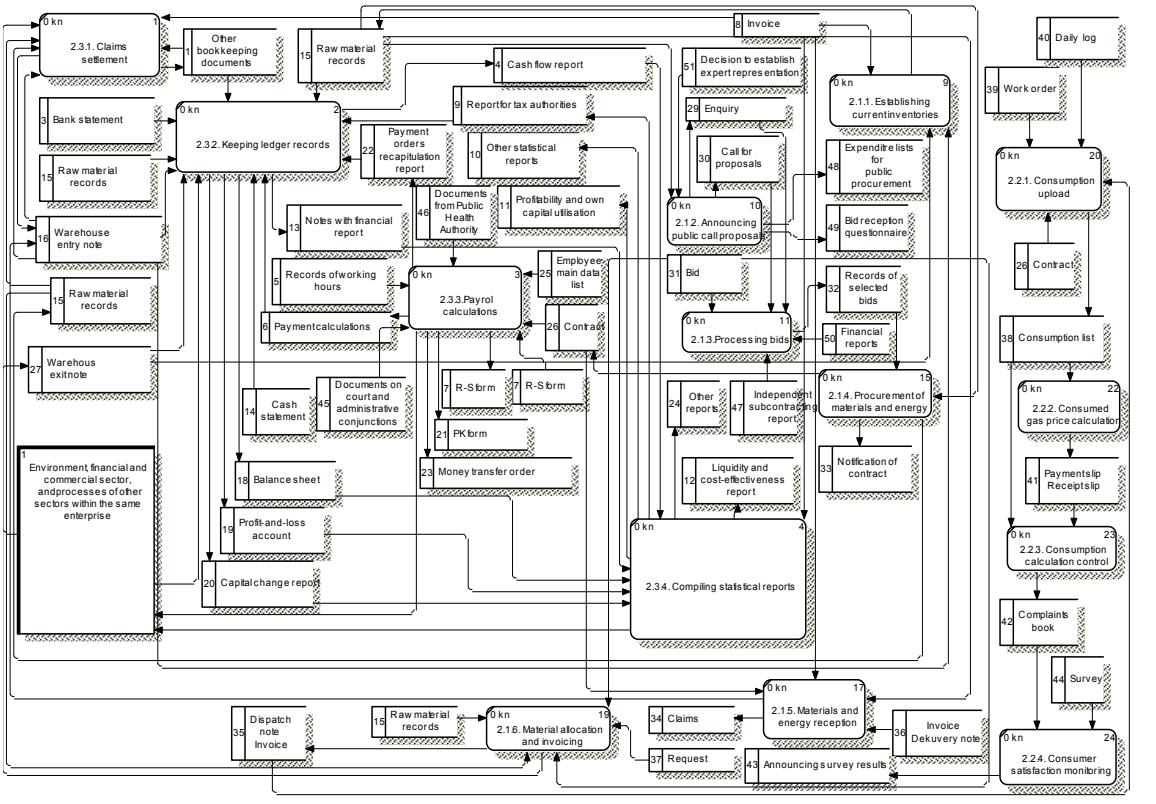


Figure 4 Data flow diagram
(The author's own design, based on the company's business logics, business rules and documents)

between them. The only problem in the proesented model is its complexity, so that it takes more time to study thus presented detailed model. Unlike models displayed earlier, the model in Figure 4 has several data flows added. As well as the P-K matrix, the data flow diagram will change depending on the change in rules of the business rules of the observed company and documents, and changes in numerous laws pertaining overall business operations.

2.3.2. Decision-making Within the Purchase Management Information System

Seamless decision-making in the purchase process requires the use of certain tools and expert system making decision based on knowledge database and fact base, with the assistance of an appropriate decision-making mechanism. The approach to decision in the purchasing process based on intiuition is quite erroneus. Decisions based on experience and intuition are connected with high risks. Decisions are made more easily in repeat purchase. When deciding on new supplieres, it is necessary to consider all the information available on the supplier, so thatthe best decision is made. Several persons should be involved in decision making in the purshasing process. Decision makin is impossible without alternative solutions. Decision-making is always related to uncertainty and risk.

3. Finance Management Information System

The purpose of the finance management information system is recording all businessevents in companies, in financial and value expression. Finance management information system and its event-recording modules are similar in numerous organisations, given that, at the end of the process, they must meet all the rules defined by the provisions of the Accounting Las. The software of the finance management information system includes the following set of modules (Figure 5): the ledger module, the analytic bookkeeping module (and other auxiliary books) comprising submodules such as accounting records of long-term assets, acconting records of invntories, raw materials, payroll, human resources receords, submodules of customers' and suppliers' balance accounts, and account records of stationery and spare parts.

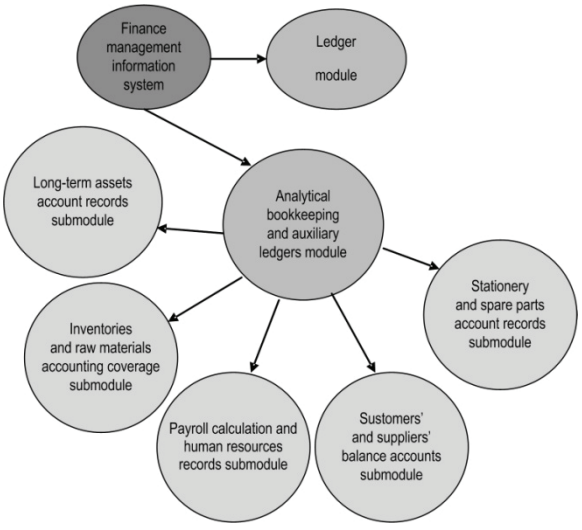


Figure 5 Information management information system architecture
(Authors' own design based on Panian & Ćurko, 2010, p. 83.)

Figure 5 shows the information management information system architecture. The key feature of the ledger module withing the accounting process is the fact that data recorded in this module refer to past events. The contents of the ledger module is determined by accounts and the chart accounts followed by the business entity. The leger module can be regarded as compulsorz, as its architectre is regulated by the Law on accountancy. At the beginning of each year, the ledger shows the initial states of assets, liabilities and capital, while accouunting events are entered into the ledger in accordance with the changes made over the year. For this some regard the ledger as a moving balance sheet, as a new balance sheet can be compiled after every recorded event, disclosing new statements of assets, liabilities and capital. The newly established statements will be a basis for compiling a balance sheet at the end of a given period.(Mamić Sačer & Žager, 2007, pp. 148-149) It is a known fact that the ledger records the company's events that initiated activities, so that it can be said that the ledger module is past-oriented. The ledger module must meet all the needs of users participating in the accountancy process. As all other modules, the ledger module can be used by several employees, i.e. all the staff with access right and authorities. Operating together with hardware and human segment of the information system, these modules primarily provide technical support to regular operation and automated progress of individual business activities featuring as a part of the above mentioned processes and subprocesses.

The ledger module also encompasses processing the company's bookkeeping documents, controlling procedures at the ledger level, and reporting from the ledger level. Bookkeping documents are compiled at the place and time of the occurrence of business events, and are first recorded in modules with auxiliary ledgers and analytic records, and only then are they entered into the ledger. In most cases, the ledger module also includes report application. (Panian & Ćurko, 2010, p. 84)

3.1. Process Accounting

Accounting includes various analysing, forecasting and planning methods and techniques. The advantage of accountancy in comparison to any other process if covering economic activities is in the fact that it can succinctly and accurately enough describe the progress of subprocesses and economic activities, as well as their results. The accounting process contains documents created by business events and transactions. The accounting process has its own outputs, created by business events and transactions. The accounting process has its outputs, i.e. processing results. Subprocesses within the accounting process are: claims settlement, ledger records, payroll calculations, compliling statisticzl reports and analysing financial reports. The claims settlement subprocess includes the following activities: controlling the form of accounting documents, controlling the textual and mathematical accuracy (of financial values). Another term most often use for claims settlement subprocess is control.Having completed the activities within the claims settlement subprocess, the documents are entered into the ledger. The activities of claims settlement subprocess are performed by the claims clerk[2]. Having completed the financial reports, the liquidator obtains certain information based on data found in the ledger. One of the tasks of the accountancy process is gathering and processing financial data from financial reports, and presenting the obtained information to the company management, supervisory board, auditors, company owners, trade unions, banks, the public, suppliers, buyers, employees and other interested persons. The Basic annual financial reports such as balance, profit-and-loss account and additional data are sent to the public, as the reports are subject to the interest of customers, suppliers, institutions, state administration and others.

[2] Activities established based on interviews with the employees of the togserved company.

3.2. The Financial Reports Analysis Subprocess

The financial reports analysis subprocess is used for the business analysis of the company, and is performed with the aim with of getting familiar with the company's financial strength. The company's success is measured so as to derive useful information for making financial decisions. The financial reports analysis subprocess is peformed for the purpose of monitoring the movement of the business success over given periods of time. The purpose of financial reporting is to meet the users needs for all required information on the company's business success. To complete a successful financial reports analysis, it is necessary to know the company's complete operation, applied accounting techniques, and the company's development strategy. Performing the reports analysis subprocess produces the output documents presenting the amounts of companies' business success. One of the company's operation success indicators is the total cost-effectiveness. The cost-effectiveness indicators show how much revenue the company has earned per unit of expenditure. Cost-effectiveness indicators are calculated based on data from the profit-and-loss account[3] created within the ledger records, i.e ledger module.

Table 2 Cost effectiveness indicator of the observed company (Indicator name: total business opearations cost-effectiveness)

DESCRIPTION	Previous year (2005)	Current year (2006)	Current year (31.12.2007)	Current year (31.12.2008)	Current year (31.12.2009)	Current year (31.12.2010)
Total revenue	112,456,446.00 kn	114,206,523.00 kn	99,405,753,16 kn	116,333,287.00 kn	133,285,526.00 kn	170,189,634.00 kn
Total expenditure	111,711,673,61 kn	114,073,431,96 kn	102,531,860,62 kn	116,254,640.00 kn	133,157,616.00 kn	169,666,688, 00 kn
OCE	1.006666916	1.001166714	0.969510868	1.000676506	1.000960591	1.003082196
Condition	The company operated cost effectively	The company operated cost effectively	The company did not operate cost-effectively	The company operated cost effectively	The company operated cost effectively	The company operated cost effectively
	99.45%	96.84%	103.21%	100.03%	100.21%	0.00%

(Author's own design based on the observed company's profit-loss-account and formulae for overall business cost-effectiveness from Žager, Mamić, Sever, & Žager, 2008, p. 193.)

Table 2 shows the cost-effectiveness of the observed company. The indicator name is overall business cost effectiveness. If the coefficient is above 1, the business operations are cost effective, if the coefficient is below 1, the business is cost-ineffective, and if the coefficient equals 1, business is on the cost-effectives limit, i.e. there is no financial result. (Ruža, Veselica, Vranešević, Cingula, & Dvorski, 2002) Table 2 shows a satisfactory cost-effectiveness coefficient for 2005, 2006, 2008, 2009 and 2010, whereas the company was cost-ineffective in 2007. as the coefficient is lower than the threshold indicator 1. In 2006, the overall business co-efficient dropped by 0.0055 in comparison with 2005. In 2007, overall business co-efficient dropped by 0.03166 in comparison with 2006. In 2008, overall business co-efficient increased by 0.031166 in comparison with 2007. In 2009 overall business co-efficient increased by 0.000284 in comparison with 2008. Table 2 shows and spells out the comment whether the business was cost-effective or not (in green cells). The formula and condition used in MS Excel 2007 are. = IF(E_n>1; "The company operated cost-effectively"; "The company did not operate cost-effectively". Based on the formula presented, the "more than" (>) comparison operator was used. If the condition was met, the result was true, i.e. the operation was cost-effective, while in the opposite case, i.e false, the operation was cost-ineffective, for the coefficient was less than 1. The overall business cost effectiveness index is calculated under with the following formula:

$$OBCEIn = \frac{OBCEn}{OBCEm} * 100$$

where

$OBCEI_n$ = overall business cost-effectiveness index

$OBCE_n$ =overall business cost effectiveness for a given period

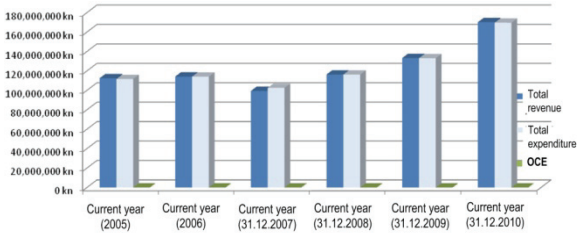


Figure 7 Company cost-effectiveness index (Index name: Overall business cost-effectiveness)

(*Author's own design based on the observed company's profit-loss-account, possibility of graph design in MS Excel and formulae for overall business cost-effectiveness from* Žager, Mamić, Sever, & Žager, 2008, p. 193.)

Figure 7 shows the cost-effectveness of overall business operations of the observed company. The index name is overall business cost effectiveness. The graph can be used for establishing whether total revenues or total revenues were higher at the end of the given year. OCE refers to overall cost-effectiveness. Overal cost-effectiveness is marked green on the diagram. The X axes represents

[3] PLA.

periods, i.e. years, whereas Y axis shows the value in Croatian kuna for total revenues and expenditures. Total expenditure that the company had are marked blue, whereas total revenues of the observed company are marked dark blue.

4. Security Management Information System

The role of the security management information system is to protect information systems within the organisation itself, their processes, and employees participating in process execution. Physical security is of utter importance in the security information system of any organisation.

It is common knowledge that the most common assaults on information systems originate from the employees themselves. In their research conducted and published in Seger & von Stroch, *Computer Crime: a Crimefighter's Handbook,* O'Reilly & Associates prove this fact. The book states that the highest ratio of security issue is caused by human error. In most cases, human errors result from inadequate alertness and employees' inadequate edcation. The second largest source of errors in information system is hardware malfunction, the third place belongs to empolyees using their position in the institution for their own personal gain, or employees using this to express their dissatisfaction or hostility to the firm or their superiors.(Kovačević, 2008)

4.1. Data Protection With Physical Procedures and Passwords

Physical protection measures include all defense measures taken to ptorect the computer instrastructure and data. Physical security is an essential part of any defence of computer infrastrcture and data. When examing computer crime, one has to take the following into account: if the criminal act was committed at the computer centre, without cracking passwords from the outside, it means that physical security was compromised, or that security measures were cracked physically, or thatthere were none. What is vital is establish exactly how the physical security of the compute environment was cracked. If the perpetrator has bypassed the technically sophisticated protection systems, it is necessary to seek the help of experts for a precisely defined area. (Bača, 2004, p. 139) If the computers or data storage media are severely damaged, the data on the media are also highly likely to be lost. In most cases, data and programs nowadays have greater value than the computers and computer infrastructure. Physical protection encompasses a set of methods and means used for protecting the information system's hardware in the broadest sense, from unauthorised approach to the system itself and using its resources, to protecting it from the impact of external events whose occcurence is unpredictable. (Dragičević, 2009, p. 81) The physical protection includes protection from thunder, rain, flood, hail, show, low temperatures, enemy forces at wartime, excessive dust, explosive devices, theft, unauthorised approach to computer assets, earthquakes, volcanic eruptions, power cuts, or possible impact of the computer itself or the storage media on hard floors. The listed protections are highly significant, as these threats may cause great material and financial marm ot the managing information systems.

Kensington locks are security systems used for protecting mice and other entry and ouptput devices from theft. If a perpetrator wants to steal the mouse, he cannot do it due to the Kensington lock, attaching the mouse to the portable computer. To protect the data in portable computers, and the computers themselves, one needs to consider the places where computers are left. Portable computers with important data should not be left in public places accessible to everyone, i.e. auditoriums, cabinets, offices and similar places, especially when these places are not provided with locks or otherwise secured against theft. Nowadays, there are clamps for locking portable computers in such a way that a perpetrator cannot open or move them, and special lockers made of solid material, where portable computers are stored so that nobody except authorised persons can open them. Quite often firms have separate and specially protected rooms for keeping computers and media for storing confiedential information. Apart from specially allocated rooms, storage media with important information can be stored in protectivee storage lockers.

Modern era has seen the development of sysems whose purpose whose aim is to raise the level of physical security, such as protectors, sensor lights, surveillance cameras, special systems for locking rooms and lockers used for storing computer equipment, alarm systems, and locators.

Table 3 shows types fo security threats to the information system. The table presents sources of threat, descriptions of domains, and specific threats, showing specifically who can harm the information system security.

Table 3 Types of security threats to information systems

Source of threat	S of domain	Specific threat
• Employees	• Neglecting to adhere to corporate security policy • Employees' errors (intentional or unintentional)	• Current employees • Former employees • Novices
• Processes	• Lack of clearly defined procedures • Lack of clearly established sequence of activities • Failure to adere to procedures • Extended process performance period	• Employees • Clients • Suppliers • Service providers • Business partners • Other public from the surroundings
• Systems	• Unforeseen hardware malfunction • Inadequate robustness of technical systems	• Technical malfunction of systems within intended use • Technical malfunction in the system due to inappropriate design or poor implementation
• External events	• Natural disasters (thunder, rain, snow, flood, earthquake, dust, storm etc.) • Disasters due to human error • Malicious actions by external actors • Negligence of external actors • Legitimate actions of external actors	• Natural events • Accidents • Malicious exernal actors • Negligent external actors • Conflicts between corporate interests and external actors

(Author's own design based on the table from Klaić, 2010.)

In companies, employees aproach to certain applications is organised as follows: the head of the department where the new employee is coming sends a request for opening a user account with data on the access level access and rights. In addition to other basic daa, the application should also include the position, job description and required access rights. When the user has received the password from the department head, he or she can change it so that he/she and the administrator can have access to certain data. Every employee meeds a password to access a specific section of the application, i.e. a spedific module. The password is usually changed monthly, and if necessary, it should be done several times a month. An optimal password should contain a minimum of seven characters – a combination of lower and upper case letters and numbers. The use of first names, surnames, names of parents, children, dates of birth, places of redince, street names etc. A chain of identical characters is also not recommendable.

When it comes to office work, the password must not be written on a paper and place in a drawer, to prevent third parties from accessing confidential data.

The most common assault at passwords is by probing or blind guesses. Blind guesses is a type of assault where the perpetrator tries to access a certain system by random guesses, with trial-and-error as the most used method. Althought this assault may seem somewhat naive, it can sometimes be effective, especially if we are familiar with the person who set the password.

When one opts for a limited number of attempts to access the computer system, the system must be set in such a way to limit the number of possible access attempts. If the user tries to access the system with a wrong pasword and username, the system should reject this person. The next option that should be plased is a message about the latest approach to e-mail, i.e. record of the latest access to data in the form of date, time and name of internet service provider. CARnet Webmail is an example of such service.

4.2. A Case of Database Damage and recovery in Finance Management Information System

Database damage may occur for several reasons, such as hardware malfunction (HDD and other storage media), or an error in the system-based program suppot. Databases can also suffer damage by malicious persons, usually referred to as hackers, by incident or accident.

Regardless of the causes of and reasons for damage, a database must be recovered to the state of preserved physical identity. Database integrity refers to true and accurate information, i.e. data contained in the base. In a broader sense, problems with database integrity include all protective measures aimed at preventing the entry of incorrect data in the electronic database. Inaccuracies and incorrect information in the database result from errors occurring during data entry or updates, program or system error, or even deliberate entry of wrong data with the intention of database damage. Databases are protected by limitations. Integrity rules are database limitations on permited states allowing mutual harmonisation between the

database and data that is entered, updated or deleted. Financial organisations work with available data, and make important decisios in accordance with this. If the data dealt with in the finance department are incorrect or have been tampered with by an invader, the consequences can be far-reaching. If, for instance, a school lost all data stored in the computer system on the employees, their years of work or salaries, the employee in the accounts department would have to re-enter all the data for each employeein the system. To retrieve the database, it is first necessary to save the data from the database on a separat medium and record all changes in the database in the log. (Varga et al., 2007, pp. 80-81)

Safeguarding the data from a database onto a medium is done by some companies every five days on the average, but this may be too seldom. It remains an open questin what would happen if a company stayed without important data in the base for five days. Any amount smaller than data lost would be profitable to invest in more frequent creation of backups. It is safer to create backups daily. It is recommendable for companies to hire their own database administrator, who would take care of backus and be resonsible for the data in the base. Database management system in a given company must be available every minute, so that 24-hour backups are possible. Backups can also be created during work.

Temporary database copies can be created within the database itself. Temporary databases can be read-only, i.e. database views. Temporary database copies record changes made in the original database. Only the values of modified pages are stored in files used for creating temporary database copies. This process is performed by using special files. If pages of the original database are modified, the server records original pages with data in a special database. This is a way of securing that only changed pages are resorded on the disk's physical space. (Lee & Bieker, 2008, p. 86) To protect all the electronic data in the base, companies use antivirus protection on personal computers and servers in finance department. Upgrading antivirus software is up-to-date. Each time a computer is used, the user must update the antivirus programme.

Hackers find it most appealing to break into banking information system, which is also a segment of the finance management information system. The reason for this, of course is that banks have large amounts of money on "their" accounts. However, as claimed by a vast majority of IT experts dealing with bank information system securities, no case of cracking a bank's information system has been recorded. Banks' information systems are under constant, daily assault, but there are no major difficulties or consequences of these attempts. The greatest problem is the "pocket impact" suffered by a banking service user if someone finds their card number and password, and can approach the bank account. When personal information, gossip or misinformation about a person is published in the media, many people believe that a psychologically balanced person will not be too upset, unless it is about finance. When it comes to users' personal property or private data on bank accounts and financial assets, the same persons will be more vulnerable, especially if an unprofessional employee discloses their personal data without the knowledge of the persons themselves or senior personal of an organisation (if it is about fabricated information). Banking information system managers must penalise such actions severely. Banking information system is the second important by importance after the military information system. Hackers' assaults at banking systems are not as common in Croatia as in other countries. Banks are currently one step ahead of potential dangers, which makes the citizens' and companies money safe.

In order to have more effective security measures in card transactions and raise the security levels of their transactions, banks must introduce Payment Card Industry – Data Security Standard (PCI-DSS) certificates, developed by the consortium of leading card companies (Visa, American Express MasterCard etc.) for more effective protection of important card data, decreasing the number of frauds, and raising security standards in companies in companies that process or store credit card data, (PCI Security Standards Council, 2010) which means banks in most case. Meeting the requirements set by PCI DSS equals effective information system risk management.

5. Conclusion

This article presents the manner of managing and functioning of the information systems of purchase, finance, information and security systems within an organisation, and their interconnectedness in the observed company. The presented models can be used by public companies involved in similar or identical activities.

Viewing the results of the financial report analysis process, according the overall cost-

effectiveness, the company did not operate const ineffectively, and neither is the overall cost-effectiveness coefficient lower than the set boundary of 1 for the strictly determined period. The company operatied cost-effectively. Thus, the conducted research has shown that, based on the sample (profit-and-loss account), there is no reason to dismiss hypothesis H_0, i.e the company's overall cost-effectiveness coefficient did not exceed the threshold between the tolerated value of 1.

The third section of this article presents te possible threeds to organisations' information systems, and describes the manners of protecting electronic information in processes, and ways of recovering electronic data in the finance management information system. Based on the description of the three information systems, one comes to a conclusion that security management information system protects data and valuable information of other information systems, and data on the outcomes of process performance. The purchase, finance, and security management systems are stand are deeply intertwined and highly important for the company management, and overall management of the company and its information data. Any company (including the observed one uses the service of the banking information system, and it is therefore very important for the observed company to have a partner bank which, among other certificates, also possesses the PCI DSS certificate.

References

Bača, M. (2004). *Uvod u računalnu sigurnost.* Zagreb: Narodne novine d.d.

Brumec, J. (2007). *Projektiranje informacijskih sustava.* Varaždin: FOI.

Dragičević, D. (2004). *Kompjuterski kriminalitet i informacijski sustavi.* Zagreb: IBS.

Ferišak, V. (2006). *Nabava-politika, strategija, organizacija, management.* Zagreb: The author's own edition.

Klaić, A. (2010). *Minimalni sigurnosni kriteriji i upravljanje rizikom informacijske sigurnosti.* Retrieved February 13, 2012 from Operacijski sustavi 2: http://os2.zemris.fer.hr/ISMS/rizik/2010_klajic/SeminarskiRad_SRS_042010_AK.pdf

Kovačević, D. (2008). *Sigurnosna politika*. Retrieved February 2, 2012 from Operacijski sustavi 2: http://os2.zemris.fer.hr/ISMS/2008_kovacevic/sigurnosnaPolitika.html

Lee, M., & Bieker, G. (2008). *SQL Server 2008.* Beograd: Kompjuter biblioteka.

Mamić Sačer, I., & Žager, K. (2007). *Računovodstveni informacijski sustavi.* Zagreb: Hrvatska zajednica računovođa i financijskih djelatnika; Ekonomski fakultet.

Panian, Ž., & Ćurko, K. (2010). *Poslovni informacijski sustavi.* Zagreb: Element.

PCI Security Standards Council. (2010). *PCI DSS*. Retrieved April 23, 2011 from IT sistemi: http://www.itsistemi.com/hr/rjesenja/sigurnosna-rjesenja/pci-dss/

Ruža, F., Veselica, V., Vranešević, T., Cingula, M., & Dvorski, S. (2002). *Ekonomika poduzeća - Uvod u poslovnu ekonomiju.* Varaždin: TIVA.

Varga, M., Ćurko, K., Panian, Ž., Čerić, V., Vukšić Bosilj, V., Srića, V., et al. (2007). *Informatika u poslovanju.* Zagreb: Sveučilište u Zagrebu.

Žager, K., Mamić, S. I., Sever, S., & Žager, L. (2008). *Analiza financijskih izvještaja.* Zagreb: Masmedia.

Vladimir Šimović
University of Zagreb
Teacher Training College
Savska cesta 77
10000 Zagreb
Croatia
Email: simovic.vladimir@yahoo.com

Matija Varga
High School Sesvete
Bistrička 7
10360 Sesvete, Zagreb
Croatia
Email: maavarga@gmail.com

Predrag Oreški
University of Zagreb
Teacher Training College
Savska cesta 77
10000 Zagreb
Croatia
Email: poreski@gmail.com