A Progressive Improvement of the Integrated System for Academic Management through Information Security Management System Audit and Metrics

Traian SURCEL, Cristian AMANCEI
Economic Informatics Department,
Academy of Economic Studies, Bucharest, Romania
tsurcel@ase.ro, cristian.amancei@ie.ase.ro

The paper presents some considerations on the possibilities of progressive approach to security issues for integrated information in an united management system - ISMS, in terms of practical use of audit techniques that meets the requirements of ISO / IEC 27001 in relation with the particular implementation of an integrated system for academic management – SIMUR, and proposes an audit mission work breakdown structure and budget for a small size university with metric for cost control.

Keywords: *Information Security Management System, IT Audit and Standards, University Information System*

1 Introduction

The reality of university information systems development reveals a number of features resulting from spiral implementation processes of applications, starting from financial accounting, grants, taxes, payroll, financial and management accounting, continuing with administrative issues, library, student accommodation, hostel and restaurant services, public auctions, services delivered by third parties and certainly the teaching, admission exams, examinations planning and conduct, catalogs, statistics, e-learning and research. In parallel with the development of IT systems, the interest in quality management and security of information processed and accessed has increased. This can be seen from the fact that besides the application of ISO 9001/2008 standard for QMS the standards ISO/CEI 27001 and 27002, together with the best practices from CobiT are applied, focused specifically on information security policy. However, it is necessary to improve information security management through proper institutionalization of the Information Security Management System concept. This complex implementation cannot be done at once due to insufficient resources, methodological flaws for this environment, shortcomings in IT education and ethical behavior of users. Overcoming these shortcomings can be done through a phased approach to improve the ISMS process within the university, by using internal audit techniques. The periodic audits are used to monitor the IT general controls and application controls system, identify threats and vulnerabilities, followed by preventive and / or corrective actions, design and implementation of remediation action plans to minimize the significant risks of university computer system. Appropriate consideration has to be given to the development of the audit mission budget, starting from the work breakdown structure of the audit mission, in order to appropriately reflect the resources involved in completing the mission.

2 Processes Map and the Structure of University Management System

Improving Information Security Management System by applying IT audit techniques, should be circumscribed from the beginning to the defined business environment through processes and interfaces of economic and social system. In the specific academic environment these processes and interfaces are grouped into three main areas: the university institutional capacity, education efficiency and quality management. Such an approach provides operational support to improve the quality of education and scientific research and is a benchmark in defining the functional architecture of the information system for university management. We applied process oriented approach mode for the academic quality management system [4] based on taking into consideration the following types of processes identified in the maps of specific university business processes university:

- the process for implementation and evaluation of services, which include labor market needs assessment for the selection of candidated thorough the admission exam, followed by curriculum development, syllabus and functions states, teaching, learning and assessment processes, final certification of teaching skills, scientific research process;
- resources related processes, human resources supply, evaluation and promotion of teachers, including the selection of associated teachers,material, financial and infrastructure resource supply and access to learning resources;
- management related processes, assessment related processes, results analysis and improvement, the academic management system in general.

The diversity of these processes and the new service requirements demanded from a performance management system, project-oriented, is reflected in the new functional coverage offered by the system through four areas covered in logic modules architecture [3]:

Fig. 1. Logic architecture

By using this logic architecture, the system will respond to a wider range of general and specific requirements, namely: the need to have access in real time to all data stored in the system, there need for electronic archiving, an overview of the educational process and financial aspects at all organizational structures levels among all

stakeholders, to give students a personal website that has all the data concerning them, for teaching and financial situation, to offer a modern interoperability support with other systems, the need to evaluate the quality of teaching process. These general requirements are met in practice by a series of services introduces by the integrated university management system, which includes: student page with new features (grades, taxes, optional classes, class schedule, exams schedule, library service), admission module, bank transaction files automatic import interface, on-line payment interface system, personnel management module, scholarship section, subscriptions, debts, integrated user identity management, digital module administration for doctoral school, postgraduate classes, statistical reports, archive, electronic catalog, diplomas, students, centralized registry, education plan, contracts, etc..To this complex functionality corresponds an appropriate technology structure such as the technology architecture modules for students from SIMUR project [1].

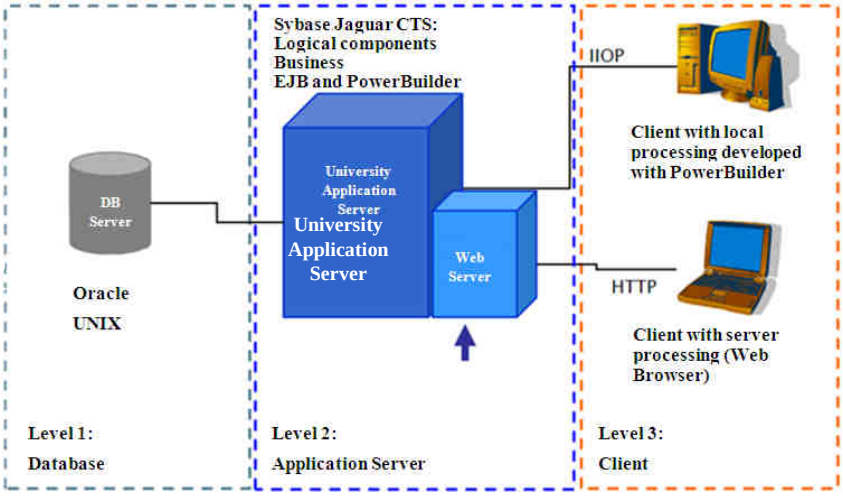

Fig. 2. SIMUR levels

By analyzing these modules we obtain the size of the complexity of information security issues that have to be processed within the integrated system of academic management which justifies based on efficiency and economy of resources reasons, the need not to extend the terms for implementation, and the progressive approach to improving the information security management system [2].

3 Information Security Management System

Information security management system is an integrated component of the university management information system that has to be addressed on two levels, technical and organizational - management plan. Under the technical aspect, in the SIMUR case the key issues of information security concerns following the same attributes of security, mainly based on CIA - confidentiality, integrity, availability, which means protection of personal data, secure storage of organization records, and intellectual property rights assurance, anywhere and anytime access for end users, students, teachers, technical staff - administrative and managerial. Under the technical aspects of information security perspective CIA

attributes has to be addressed through the application of controls, controls consistent with the design methodologies and software customization settings, supported by operating systems, software packages and systems management database ERP and BI. Beside this, quality controls systems for data input to ETL, data output and database integrity checks has to implemented through automatic controls, substantive or individual, joint or linked, dynamically configurable controls and interfaces controls with external systems, for data import or export [5].

In the organizational plan, the experience recommended by best practices emphasizes that we must focus on defining, implementing and enforcing security policies at the university level, for clear allocation of security responsibilities from top management level and up to student level. Not only information security responsible has to be trained and evaluated, but also regular users of the system such as students, also confidentiality agreements, internal rules and administrative measures had to be implemented to comply with information security policy strongly promoted by the university. This goal competes in a sustained marketing activity to strengthen information security and the IT culture based on clear understanding of the university vulnerabilities, threats and security risk management to reduce their negative impact not only on the image and on material resources and financial resources of the university.

4 Application of audit technologies

IT audit aims to highlight the lack of control procedures or the lack of efficacy when they were poorly designed or improperly applied. IT audit seeks those security breaches due to deficiencies of security policy and controls system, proposing corrective measures and actions to minimize the impact of security risks. Implementation of quality management system - QMS is a significant step for the discipline of system base activities and information system. By respecting the requirements of ISO 9001/2008 we have available system procedures to control documents and records, controlling a number of non-compliances and operational procedures that support business functionality for academic processes. In the area of information security issues a remarkable effort has been put in to define a security policy but is not integrated into a unified security management system. In an effort to win in the effectiveness area we must adopt a strategy of gradual ISMS improvements by removing non-conformities identified through an audit plan centered on the IT system. The audit plan must be reported as appropriate to the requirements expressed by the ISO/IEC 27001/2005. The first priority is security policy review to ensure compatibility requirements required by the new configuration of the integrated management system connected to the new provisions of education law.

The next step should be a professional approach to resource management by documenting the implementation rules for information and processing equipment ownership and acceptable use rules. Physical and working environment security must be enhanced significantly by firm controls aimed at the organization and operation of physical and security perimeters, covering physical access control, mode of work in public access areas and especially the protection against external environment threats: fires, floods, earthquakes and deliberate human destruction. The increased

dependence of the teaching process, the act of teaching, seminars, assessment and examination on the proper functioning of university computer networks requires special equipment safety audits, from preventing incidents to utilities supply, e.g. electricity, to the proper maintenance, computer servicing. The use of audit controls must be applied in the management of change, due to high number of changes and of professionals involved in their implementation. Here comes the factor of IT team volatility, in general, not only in academic environment, which required the outsourcing of the SIMUR project. One of the particularities of educational information, namely the need to archive a long time, now adds classic archives and electronic archives. But in addition to the records of teaching, catalogs, files and registry records, electronic archiving is considering the backups of databases and major software products. These backups and other organizational measures should be included in a disaster recovery plan DRP component of business continuity plan BCP. Although BCP is not the size of importance, as those in the field as banking of insurance industry, however, if we take into consideration the fact that many people come back after many years to the university archives for information, we appreciate that a BCP is justified.

5 Business Continuity Process

An effective business continuity processes and procedures are based on documented, tested and updated. Predefines business continuity plans and resources necessary actions to achieve the plan, allowing an organization to minimize disruption to its operations where one or more systems, critical procedures are interrupted due to a natural disaster, accident or act of sabotage. PCA must provide solutions to break the normal process of business, destruction or loss of data. It must cover the time between initial response and the resumption of normal operations and are based on approved business continuity strategies.

The organization must ensure continuity of its core activities in the event of a disaster or significant interruption of a critical task. Continuity and recovery strategies are based on the concept of ensuring the availability of all key resources that support key business processes in concert with the organization's needs and consistent with the level of service stipulated in contracts with third parties [6].

The proposed model includes four steps:

- first step is performed PCA implementation project planning, requirements definition and analysis organization for coverage of the PCA, in terms of processes and applications that are included in the end;
- in the second step to move to implementation of project activities, design and implementation of PCA, including the setting up of idle time for each process, including for application;
- the next step is to test and verify continuity plan to verify the effectiveness of the restoration processes and applications included in the end, during the period set out in the strategy, for a complete verification plan, testing must be done by stopping all processes and applications included in the end, in order to check the interrelationships between them;
- the last step which mainly undertakes to update and improve business continuity plan to ensure continued maintenance.

These steps include risks that the auditor must verify through audit procedures, such as the plan developed should include all

processes and applications as defined by management decision, the maximum downtime should take into account the interrelationships between all organization and processes not only within the scope of the processes, testing plan must be made by applying the worst case scenario and applying the interruption of all processes, processes and emerging applications in the organization since the last update of the plan must be identified and analyzed.

Implementation of BCP for the entire organization includes several important activities:

- for the plan to operate if a disaster procedures, personnel organization should understand what their respective roles and responsibilities;
- distribution of documents the business continuity plan should be a strictly controlled process, BCP contains information on contact details, details of connecting to the organization's IT equipment which are regarded as confidential;
- initiation of maintenance plan should be clearly defined to ensure that no changes take place without consultation with all parties connected with this process.

The changes in the organization after the continuity plan has been developed will be analyzed in terms of impact on processes covered by the plan, in case of changes with major impact on organization processes necessary to recover the business risk analysis, or persons or positions involved in the plan, which left the company or have undergone changes in duties. The auditor has to verify that all the changes have been implemented in the plan.

6 Audit Mission Budget

The audit mission budget is obtained by estimating its components, and starts with the entries in of the cost estimates:

- the purpose of the audit mission includes a description of acceptance criteria, key deliverables, assumptions and constraints of the engagement; one of the basic assumptions that should be considered when estimating the costs of the mission, is whether the estimates are limited to direct costs, or if estimates include also the indirect costs, indirect costs are costs that can not be traced directly to a specific mission and, therefore, are accumulated and allocated more equitably on the audit missions performed during a certain period (usualy 1 year);
- the most common constraints for many audit missions concerns: budget, delivery dates, available skilled resources and organizational policies; the detailed work breakdown structure include the relations between different components of the mission and deliverables, including time and resources allocated for each phase; additional information can be found in purpose audit engagement, including contractual and legal requirements, insurance, intellectual property rights and licenses, all this information is taken into account when developing cost estimates;
- mission planning, the type and amount of resources and the length of time that these resources are used to accomplish the mission, are major factors in determining the cost of the engagement; estimating activity resources involves determining the availability of personnel and systems necessary to perform the activities of the audit program, audit engagement planning review detailed work breakdown structure to verify the adequacy of duration and resources;
- identify the necessary human resources

audit engagement, to be available and have the knowledge, experience and skills, specific mission; where the organization lacks the necessary resources, will identify external suppliers or internal (within the group) lack resources.

In order to estimate the cost of an audit engagement we have used an audit mission for certification in accordance with the requirements of ISO 27001 of a small size university with approximately 200 system users, whose detailed work breakdown structure was made on the basis of research and experience gathered in the field of IT audit, presented in Figure 1. Estimation in terms of timing of the work is included in the detailed structure for the work to be done in a medium university, taking into account that for each activity is assigned a team of two people: a senior auditor shall have half the time for each activity, and a junior auditor.

	Task Name
1	**1. Stage 1 - Documentation Review**
2	1.1 ISMS Scope
3	1.2 Information Security Manual
4	1.3 Risk Methodology
5	1.4 Risks Evaluation Report
6	1.5 Risk Treatment Plan
7	1.6 Controls Efficiency Measurement Procedure
8	1.7 Statement of Applicability
9	1.8 Roles and Responsibilities for ISMS
10	1.9 Security Incident Management Procedure
11	**1.10 ISMS Specific Procedure**
12	1.10.1 Documents Control Procedure
13	1.10.2 Records Control Procedure
14	1.10.3 Internal ISMS Audits Procedure
15	1.10.4 Corrective and Preventive Action Procedure
16	1.10.5 Management Review Procedure
17	**1.11 Procedures and Controls Support for ISMS**
18	1.11.1 Security Policy
19	1.11.2 Organization of Information Security
20	1.11.3 Asset Management
21	1.11.4 Human Resources Security
22	1.11.5 Physical and Environmental Security
23	1.11.6 Communications and Operations Management
24	1.11.7 Access Control
25	1.11.8 Information Systems Acquisition, Development and Maintenance
26	1.11.9 Information Security Incident Management
27	1.11.10 Business Continuity Management
28	1.11.11 Compliance
29	1.12 Stage 1 Closing Meeting
30	**2. Stage 2 - Implementation Audit**
31	2.1 Asset Management
32	2.2 Human Resources Security
33	2.3 Physical and Environmental Security
34	2.4 Communications and Operations Management
35	2.5 Access Control
36	2.6 Information Systems Acquisition, Development and Maintenance
37	2.7 Information Security Incident Management
38	2.8 Business Continuity Management
39	2.9 Compliance
40	2.10 Audit Closing Meeting

Fig. 3. Audit Mission Work Breakdown Structure

Based on previous experience it was established that in addition to the hours included in the work breakdown structure, we have to plan 20 additional hours for each team member to complete the engagement documentation and 10 hours from an expert in ISO 27001. The activity on the project is coordinated by a project manager who is allocated 10 hours for each phase of the project. In terms of costs for times as necessary in this mission, we recommend the use of cost standards for each hour of the persons involved. These are the assumptions underlying the proposed construction budget.

The business carried out within the time limits, depends on the capacity and expertise of auditors involved in the audit engagement. A performance evaluation scheme rewards those who submit quality reports within the constraints of time.

In addressing the audit engagement there are two different views [7]. One approach is to conduct full audits by analyzing the areas included in the scope, regardless of how long it takes this operation, the extension of hours budgeted for the implementation of additional testing required and the inability to provide timely audit opinion. Another approach is that the audit mission management establishes a defined number of hours depending on the level of risk for the processes audited. If the budget expires, the

management audit reviews the mission's unfinished areas and decides any extensions or changes in procedures undertaken.

The most common problems encountered in an audit budgeting, consists in anticipating the time the audited organization will respond to the audit team (scheduling meetings, providing documentation). In order to anticipate of these problems expertise is required in managing the budget of the audit mission.

Based on the hypothesis made during the cost estimation and detailed work breakdown structure shown in Figure 3 for a certification audit engagement in accordance with the requirements of ISO 27001, following budget has been prepared:

Table 1. Audit Mission Budget

Stage / Activity	Position Involved	Effort (men-hours)	Hourly Rate (RON)	Fees
1. Documentation Review		126		25.500
Activities 1.1-1.9	Assistant Auditor	36	150	5400
	Senior Auditor	18	200	3600
1.10 ISMS Specific Procedures	Assistant Auditor	10	150	1500
	Senior Auditor	5	200	1000
1.11 Procedures and Controls Support for ISMS	Assistant Auditor	28	150	4200
	Senior Auditor	14	200	2800
	Expert	5	600	3000
	Manager	10	400	4000
2. Implementation Audit		130		26.500
Activities 2.1-2.10	Assistant Auditor	50	150	7500
	Senior Auditor	25	200	5000
	Expert	5	600	3000
	Manager	10	400	4000
Documentation Completeness	Assistant Auditor	20	150	3000
	Senior Auditor	20	200	4000
Total Fees				**52.000**
Expenses				3000
Project Total				**55.000**

The budget developed is verified and sent for approval, because it will be subsequently used as a baseline for reporting project efficiency.

Cost control is the process of monitoring the status of the project to update the project budget and manage the changes to the original costs. Updating budget involves recording the actual costs incurred up to date. Any increase in the approved budget must be approved by responsible persons who approved the initial budget.

Tracking expenditures made without regard to value the work that led to these charges, has a low value for the project because it allows only the monitoring of enrollment in the approved budget. The most important steps in cost control are undertaken to analyze the relationship between work phases, stages of the project completed and costs incurred.

Project cost control includes:

- analysis of the factors that create changes to the original cost;
- timely review of all applications for amendments to the original specifications, in terms of additional costs incurred;
- approved change management when they occur;
- ensuring that expenditures do not exceed the approved budget, at the time and the level of total project;

- monitor performance in terms of cost, to isolate and understand the difference to the original approved cost;
- monitoring of work performance against costs incurred;
- preventing the inclusion of unapproved changes in reported costs or resource use;
- inform stakeholders about the changes approved and their associated costs;
- implementation of actions to keep the cost overruns within acceptable limits.

Control project costs for the search for causes positive and negative variations from the original approved budget.

7 Metrics for cost control

Cost control during the audit mission is performed by evaluating the cost variation and plan variation indicators, and analysis of the correlation between them.

Plan variation VPL is a measure of the plan performance assessed at the audit activity level:

$$VPL_i = VD_i - VP_i$$

where:

VD_i - gained value for audit activity i;

VP_i - planned value for audit activity i.

$$VD_i = VP_i * \frac{\sum_{j=1}^{m} TE_j}{\sum_{k=1}^{n} TP_k}$$

where:

TE_j - tests performed during activity i;

TP_k - tests planned during activity i.

The tests performed during audit activity represent the number of items to be verified for each risk (1 item for automatic controls or 10% of the population and no more than 29 items), considering that the verification of each item is equal on average.

The cost variation CS is another measure of the audit mission performance at audit activity level:

$$CS_i = VD_i - CR_i$$

where:

VD_i - gained value for audit activity i;

CR_i - real cost for audit activity i.

$$CR_i = \sum_{j=1}^{n} \frac{HC_j}{HP_j} * TH_j$$

where:

HC_j - hours utilized for activity i tests;

HA_j - hours planned for activity i tests;

TH_j - hourly rate for audit team members;

n - number of audit team members.

If the cost variation is positive that the planned costs are exceeded, situation that must be analyzed to determine the causes that led to these overruns.

During the audit engagement there is a direct correlation between the plan variation and cost variation. If $CS_i > VPL_i$, the work performed is carried out better than was planned. If $CS_i < VPL_i$, then the planned budget is exceeded or the deadline of the activity i is exceeded.

The tracking of these indicators and the analysis of the correlation between them is carried out weekly by the audit mission manager based on the reports received from the audit team and checks carried out on the engagement status.

8 Conclusions

Through the progressive improvement of the ISMS, audit techniques have the effect of reducing control risk and detection risk encountered during audit mission conduct. The mitigation of control risk is performed to avoid situations in which errors that can have a significant impact cannot be prevented and corrected in time. Delays, especially those encountered due to improper procedures for

notification and resolving of security incidents are the main problem in this case. Detection risk is more frustrating because the controls system could not detect at all certain errors that significantly affect the image and the proper functioning of the organization. Taking into account all these considerations on improving information security will enhance the prestige of the university with high confidence level. The work breakdown structure of the audit mission is developed in detail for each audit mission in order to have a good instrument that can be used for audit mission tracking during engagement fieldwork.

References

[1] A. R. Bologa, R. Bologa, Gh. Sabau, M. Muntean, "Integrated Systems in higher education," *WSEAS Transactions on Computers*, Volume 7 Issue 5, Wisconsin, USA May 2008.

[2] A. R. Bologa, T. Surcel, C. Amancei, "Major Risks in Implementing an ERP System in Universities", *Access to Quality*, 11th Volume, no. 113, Editura Cibernetica MC, Satu Mare, 2010.

[3] M. Muntean, Gh. Sabau, A. R. Bologa, T. Surcel, A.Florea, "Performance Dashboards for universities," *2nd International Conferenc eon Manufacturing Engineering, Quality and Production Systems MEQAPS'10*, Constanta, Available at: http://www.wseas.us/elibrary/conferences/2010/Constantza/MEQAPS/MEQAPS-36.pdf, 2010

[4] M. Olaru, R. Sarbu, *Quality manual*, ASE 2008.

[5] A. M. Suduc, M. Bîzoi, F. G. Filip, "Audit for Information Systems Security," *Informatica Economica*, vol. 14, no. 1, 2010.

[6] M. Popa, C. Toma, C. Amancei, "Characteristics of the Audit Process for Distributed Informatics Systems," *Informatica Economica*, vol. 13, no. 3, 2009.

[7] K. H. S. Pickett, *The Internal Auditing Handbook*, third edition, John Wiley&Sons, Chichester, 2010.

Traian SURCEL is Professor at Academy of Economic Studies Bucharest, Faculty of Economic Cybernetics, Statistics and Informatics, Department of Informatics in Economy, PhD in Economic Cybernetics from 1987. He coordinates the Fundamentals of IT&C for Business Management professors group and also PC Laboratories for Faculty of, Marketing, Commerce and International Business and Economics. Hi is Internal Auditor for the ASE Bucharest. His main research areas are: information system and database analyze and design, IT systems audit, e-Learning applied methodology, IT&C for Business Management.

Cristian AMANCEI is University Assistant at Academy of Economics Studies Bucharest, Faculty of Economic Cybernetics, Statistics and Informatics. He is a PhD candidate from October 2007 at Economic Informatics Department from Academy of Economic Studies. He holds a Master in Science – Computerized Project Management from Academy of Economic Studies, Bucharest. He is Certified Information Systems Auditor (CISA). He graduated in Economic Informatics at Faculty of Economic Cybernetics, Statistics and Informatics in 2006. His main research areas are: information system audit, data structures, metrics in information systems, IT controls and IT risks.