Information Security of University Information Systems

Viljan Mahnič[1], Janko Uratnik[2], und Natasa Zabkar[3]

[1] University of Ljubljana
Faculty of Computer and Information Science
Trzaska 25, SI-1000 Ljubljana, Slovenia
viljan.mahnic@fri.uni-lj.si
[2] Dergomaska 53, SI-1000 Ljubljana, Slovenia
juratnik@email.si
[3] Celovska 269, SI-1000 Ljubljana, Slovenia
nzabkar@email.si

Abstract The aim of this paper is to give some recommendations for the improvement of the level of information security of university information systems. For this purpose two standards/guidelines are presented: COBIT/ISACF and BS 7799. COBIT is an open system that includes guidelines for implementation and evaluation of information technology control. BS 7799 is a closed system which includes guidelines for ensuring information security. These standards/guidelines are recommended by the Bank of Slovenia as the Slovenian financial supervisory institution. We discuss the possibility of using the experience from financial institutions in the implemention of security standards in university information systems. At the end of the paper some recommendations are given.

1 Introduction

The security of a University information system (UNIS) is of great importance, as has been discussed at the 7^{th} International Conference of European University Information Systems (EUNIS) 2001 (Berlin) [Mo01], [Fr01]. This has been for some time recognized by the universities in the United States of America, where many universities publish the security policies and procedures on their home pages [Co02a].

In Slovenia, the auditing of information systems is mandated by law for banks (since 1995), brokerage houses (since 2000) and insurance companies (since 2001). One of the auditing areas is information security. In this paper we shall try to apply experience from auditing the security of financial information systems in Slovenia, such as banks and insurance companies, to UNIS.

Banks have a long tradition in providing security for their information systems. The Bank of Slovenia is the supervisory institution that monitors the security of information systems of all banks, domestic and foreign, in Slovenia. There are two standards/guidelines recommended in the Report on Supervision of Banking Operations in the Year 2000 and the First Half of 2001 by the Bank of Slovenia [Ba01]:

- COBIT/ISACF (Control Objectives for Information and Related Technologies / Information Systems Audit and Control Foundation) [COBIT-AG, CO, MG] and

- BS 7799:1995 ”Code of practice for information security management” [PSIST-BS 7799].

In this paper we shall discuss the possibility of using these standards/guidelines in UNIS.

2 Security standards/guidelines for information systems

2.1 COBIT

COBIT[1] is an open system that includes guidelines for the implementation and evaluation of information technology controls for meeting fiduciary, security and quality requirements. It is an IT governance tool that helps management to balance risks and control investment, users to get assurance on the security and control of IT services, and auditors to substantiate their opinion on internal controls.

COBIT has three vantage points ("COBIT cube", figure 1):

- information criteria (fiduciary, security and quality requirements);
- information technology (IT) resources (data, application systems, technology, facilities, people) and
- IT processes (planning and organization, acquisition and implementation, delivery and support, monitoring).

Information needs to conform to information criteria in order to satisfy business objectives. Apart from information criteria, COBIT can be used for assessing IT resources as well as IT processes. There are 34 processes and 318 detailed control objectives [Is00b], grouped into four domains:

1. PO: planning and organization (IT Strategic Balanced Scorecard; strategy and tactics, compliance of the information architecture and business strategy, organizational and technological infrastructure);
2. AI: acquisition and implementation (IT Development Balanced Scorecard; identification, development/acquisition, implementation and maintenance of IT solutions);
3. DS: delivery and support (IT Operational Balanced Scorecard; actual delivery of required services, service level, security, continuity, training, application controls), and
4. M: monitoring (Balanced Business Scorecard; assessment of the quality of IT processes and their compliance with control requirements, independent assurance from internal/external audit).

[1] COBIT has 6 parts: Executive Summary, Framework, Detailed Control Objectives [Is00b], Management Guidelines [Is00c], Audit Guidelines [Is00a] and Implementation Tool Set. COBIT is available for download at www.isaca.org.

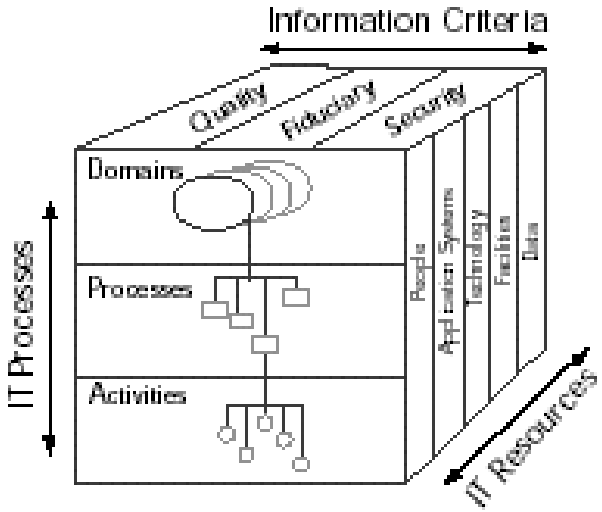

Figure 1: COBIT cube [Is00b][2]

Domains PO and M deal with planning and monitoring IT strategy, while domains AI and DS deal with delivering of strategic IT goals. Security is considered in process DS5: "Ensure systems security".

For each process the guidelines for assessing the maturity level are given [Is00c] as well as the guidelines for assessment and auditing [Is00a]. One possible way of using COBIT is to:

1. Select the most important control processes and control objectives from [Is00b] (for example the process DS5: "Ensure systems security);
2. Assess the current level of maturity for each selected process using [Is00c];
3. Monitor the progress toward the desired level of maturity using the indicators from [Is00c];
4. Periodically audit the selected processes using [Is00a].

The use of COBIT has already been presented in [MZ00], so in this paper we shall introduce only how COBIT (third edition) can be used for reaching compliance with Slovenian law requirements [SZ01].

Slovenian regulations define the contents of an audit report on the quality of information systems in banks (Official Gazette of the Republic of Slovenia No 6/1995), brokerage houses (Official Gazette of the Republic of Slovenia No 6/2000) and insurance companies (Official Gazette of the Republic of Slovenia No 6/2001). According to these regulations

[2] Copyright 1996, 1998, 2000 Information Systems Audit and Control Foundation. Reprinted with the permission of the Information Systems Audit and Control Foundation and IT Governance Institute.

the audit report must include opinions and recommendations about the following five areas of IT:

1. **Compliance of the information system with the business goals;**
2. **Efficiency of the information system;**
   These two areas can be compared to the COBIT quality requirement, which is defined as a combination of effectiveness and efficiency.
3. **Policy and organization of the security and protection of the information system and data;**
   This area can be compared to the COBIT security requirement, defined as a combination of confidentiality, integrity and availability. They can also be compared to the COBIT fiduciary requirement, defined as a combination of compliance and reliability of information.
4. **Appropriateness of the general, system and other controls;**
   Appropriateness of general, system and other controls can be compared to all COBIT requirements, so it is more appropriate to use a comparison with COBIT-IT processes approach.
5. **Technology.**
   Technology is one of the COBIT-IT resources, so the approach through IT resources seems to be the most appropriate for the comparison, although the COBIT-IT processes approach could also be used (process PO3: "Determine Technological Direction").

In our opinion, the same requirements are applicable to the academic environment. In this case the ”business goals” would be replaced with ”university goals”, and the COBIT guidelines could be followed.

2.2 BS 7799: 1997 Code of practice for information security management

The information security management is one of the most important issues of information systems governance. The objective of the information security efforts is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. BS 7799 is the code of practice for information security management and implementation in information systems.

Information security management has three basic components:

- **Confidentiality** (protecting sensitive information from unauthorized disclosure or intelligible interception);
- **Integrity** (safeguarding the accuracy and completeness of information and computer software);
- **Availability** (ensuring that information and vital services are available to users when required).

Control objectives described in BS 7799 deal with all aspects of information security threats which also exist in a university environment and in UNIS.

The controls are divided into ten sections and some of them can be specified as key controls, which are applicable to any IT environment:

1. **Security policy**
   The management direction, responsibility allocation and support for information security is of vital importance in achieving the described security objectives. It needs to be expressed in a written security policy, which must then be accepted and implemented.
2. **Security organization**
   Information security is the management's responsibility and the areas of responsibility should be clearly stated. Security of third party IT systems can have effect on organizational IT systems, therefore security requirements should be included in the third party contract.
3. **Assets classification and control**
   The owners of the assets should be identified for major assets. Various IT assets are of different importance for the university and they should be classified by their owners and labeled accordingly.
4. **Personnel security**
   Personnel is very important for the security of IT systems, so the human resources department needs to take this into account when selecting new employees. Confidentiality agreement should be signed by each employee and security training and education should be implemented.
5. **Physical and environmental security**
   The most evident and perhaps the easiest to implement is the physical and environmental security. It should protect the IT facilities from unauthorized access, damage and interference. The fact is that the IT facilities are not a show room accessible to anybody and that they need an appropriate fire, water, dust and other possible environmental damages protection.
6. **Computer and network management**
   Appropriate procedures required to manage and operate computer and network facilities, regardless of the size of the organization, have to be specified, documented and implemented. Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to all kinds of security incidents. Software development activities, which are interesting and popular with the students in a university environment, should be separated from production facilities.
7. **System access control**
   Logical or system access control is another important objective to be reached. The need of the user to access the information system has to be properly specified according to the access policy, authorized by the responsible management, segregated according to the user roles, monitored and supervised. Proper user name and password policy and its implementation, audit trails recording - logs and their regular control are necessary to achieve this objective.
8. **Systems development and maintenance**
   Proper system development should ensure that security is built into an IT system prior to its use, therefore the security measures have to be specified in the software and system development stage. Data and processing need to be validated and in some cases encrypted.

9. **Business continuity planning**
   Business continuity and disaster recovery planning has an increasing importance in IT governance; therefore it has to be carefully planned and regularly tested.
10. **Compliance**
    Non-compliance of the information system and its operations with legal and contractual requirements can represent an important risk for any organization and for the university as well.

A university and its UNIS can be considered as any other organization as regards information security. It needs a well-specified security policy based upon a code of practice, and its implementation in the information system, which will than provide secure, efficient and effective transactions to the users.

3 Information security of UNIS

COBIT and BS 7799 do not have limitations regarding their use in an academic environment. We believe both of them can be used in UNIS for fulfilling fiduciary, security and quality requirements.

Financial institutions deal primarily with financial transactions. Universities deal with different transactions, such as: enrolment in the academic year, student scheduling, applying for examinations, providing information about grades, exam dates, diploma thesis, masters thesis, fees payment etc. In this paper, we have defined three different types of university transactions:

- **Financial transactions:** deal with finance, they are similar to transactions with banks (BANIS) and therefore need similar treatment (fees, books, library etc.);
- **Privacy transactions:** contain personal data, as defined in the Data Protection Act of the Republic of Slovenia http://www.sigov.si/mp/, these data need to be logically and physically secured in order to ensure compliance with the Data Protection Act (enrollment, grading information, e-mail, e-library etc.);
- **Information transactions:** do not include financial or personal data, they are primarily requests for information, such as curriculum, subject description etc, the primary requirement for this type of data is not security or fiduciary requirement, but quality requirement: efficiency and effectiveness (e-learning, e-curriculum, e-scheduling etc).

Financial transactions demand higher level of security than privacy transactions. Information transactions need to be correct and fast, while security is of less importance. Therefore, BS 7799 is more appropriate for financial and privacy transactions and COBIT is more appropriate for information transactions (Table 1).

Implementing COBIT and BS 7799, as any other project, demands time and resources. One of the key factors for project success is to gain management's support.

A possible starting point for building security awareness is to develop information security policy for UNIS by following:

- COBIT management guidelines for the process DS5: "Ensure Systems Security" [Is00c];

	Type of University transactions	COBIT	BS 7799
1	Financial transactions		ok
2	Privacy transactions		ok
3	Information transactions	ok	

Table 1: *Security standards/guidelines for UNIS*

- BS 7799 guidelines in the section 1.1.1: ”Information security policy document” [Bs97].

According to COBIT, one of the critical success factors for the process DS5: ”Ensure Systems Security” is the existence of an overall security plan that includes the building of awareness, policies and standards, implementation guidelines and monitoring. The effectiveness of this plan is measured through key goal indicators, such as ”no incidents causing public embarrassment”. The efficiency of this plan is monitored through key performance indicators, such as: ”reduced number of security incidents”, ”amount of downtime caused by security incidents” etc. In the maturity model, level 0 (non-existent) is characterized by no need for IT security, while at level 5 (optimized) IT security requirements are clearly defined, optimized and included in a verified security plan.

According to BS 7799, the information security policy document should be issued by top management team. It should contain definition of information security, a statement expressing management’s support, an explanation of specific security policies, a definition of responsibilities for information security and an explanation of the reporting process for security incidents.

When designing information security policy, experiences of other universities, such as Cornell University, could be taken into account. At their home page we can find "Policy regarding responsible use of Electronic Communication" [Co02a]. For example, in their policy they specify the procedures for dealing with ”downloading or posting to university computers, or transport across university networks, material that is illegal, proprietary, in violation of university contractual agreements, or otherwise is damaging to the institution”. They also provide ”Control Self Assessment Guide for Information Technology” [Co02b], prepared by their internal audit department.

Since UNIS is part of academic environment, students creativity could be used as additional resource. The curriculum could be modified ([MZ01], [JZ01]) so that students would learn what to expect from the security of information systems and how to build secure information systems. Their research could be directed toward developing propositions for specific elements of UNIS information security policy. Initiating projects at the university that would involve information systems auditors (CISA) and IT security professionals from financial and other institutions would facilitate transfer of knowledge about security solutions for information systems.

4 Conclusion

University information systems (UNIS) and financial information systems have different levels of security. Regulation is tighter for financial information systems. In this paper we

have tried to apply experience from the area of security in financial information systems to the area of security of UNIS.

When developing and auditing security of financial information systems, international standards/guidelines such as COBIT and BS 7799 are recommended by the Bank of Slovenia as the Slovenian financial supervisory institution. These standards/guidelines provide a systematic approach for implementing and auditing security controls for information systems in general, including UNIS.

A possible start for improving the security of UNIS is to:

- follow COBIT management guidelines for control process DS5: "Ensure Systems Security" and
- follow BS 7799 guidelines for section 1.1.1: "Information security policy document".

This would help building security awareness at the university management's level, so their support would be guaranteed through the (long) process of developing informational security for UNIS.

In this paper we have considered two standards/guidelines. Our solution could be improved by also using other standards/guidelines, as well as using experience from other countries.

References

[Ba01] Bank of Slovenia: Report on Supervision of Banking Operations in the Year 2000 and the First Half of 2001 http://www.bsi.si/html/eng/publications/nbp/NBP-Report00-01ang-internetvse.pdf>, 11.2.2002

[Bs97] PSIST BS 7799:1997 (BS 7799:1995): Code of practice for information security management. Urad Republike Slovenije za standardizacijo in meroslovje, Ministrstvo za znanost in tehnologijo, Slovenia, 1997.

[Co02a] Cornell University: Policy regarding responsible use of Electronic Communication http://www.univco.cornell.edu/policy/RU.html, 11.1.2002

[Co02b] Cornell University: Control Self Assessment Guide for Information Technology http://www.aff.cornell.edu/audit/csa/info-tech.html, 11.1. 2002

[Fr01] Franck O.: An experiment in security at the University of Poitiers. In (Knop J., Schirmbacher P.) Proc. 7^{th} International Conference of European University Information Systems (EUNIS), Berlin, Germany, 2001. Humboldt University, Berlin, 2001; pp 97-102.

[Is00a] ISACF: Control Objectives for Information and Related Technology (COBIT), Audit Guidelines. Information Systems Audit and Control Foundation (ISACF), USA, 2000 www.isaca.org

[Is00b] ISACF: Control Objectives for Information and Related Technology (COBIT), Control Objectives. Information Systems Audit and Control Foundation (ISACF), USA, 2000 www.isaca.org

[Is00c] ISACF: Control Objectives for Information and Related Technology (COBIT), Management Guidelines. Information Systems Audit and Control Foundation (ISACF), USA, 2000 www.isaca.org

[JZ01] Javornik M.; Zabkar N.: Information Systems Auditing Education in Slovenia: Results of Preliminary Research. In: Proc. 9^{th} Conference of Audit and Control of Information Systems, Otocec, Slovenia, 2001. Slovenian Institute of Auditors, Ljubljana, Slovenia, 2001; pp 53-74.

[MZ00] Mahnic V.; Zabkar N.: The Role of Information System Audits in the Improvement of University Information Systems. In Proc. 6^{th} International Conference of European University Information Systems (EUNIS), Poznan, Poland, 2000; pp 101-110.

[MZ01] Mahnic V.; Zabkar N.: Education in IT controls at the Faculty of Computer and Information Science in Ljubljana. In (Knop J., Schirmbacher P.) Proc. 7^{th} International Conference of European University Information Systems (EUNIS), Berlin, Germany, 2001. Humboldt University, 2001; pp 168-172.

[Mo01] Morris F.: "Enhancing Information systems security in an academic organization". In (Knop J., Schirmbacher P.) Proc. 7^{th} International Conference of European University Information Systems (EUNIS), Berlin, Germany, 2001. Humboldt University, 2001; pp 92-94.

[SZ01] Susnjar G.; Zabkar N.: Audit and control of Electronic Documents Management Systems. Workshop papers, Otocec, Slovenia, September 27, 2001. Slovenian Institute of Auditors, Ljubljana, 2001; Slovenia