IT Governance and security: ISO 27000 at Universitat Jaume I

Ricardo Borillo[1], José Pascual Gumbau[2], Vicente Andreu Navarro[3], Andrés Marzal[4], and Paúl Santapau[5]

[1]borillo@uji.es, Computing Services.
[2, 3, 5] Office for Planning and Technology Forecast.
[4]Vice-Chancelor of Campus, Infrastructure, and New Technologies,
Universitat Jaume I, Avinguda de Vicent Sos Baynat, s/n, 12071 Castellón, Spain

Keywords
IT Governance, ISO 38500, ISO 27000, Security, ISMS, software life-cycle.

1. Introduction

The role that IT systems play at universities has been increasing on importance during the last years. In almost every field of the university management there is an IT solution present (on-site classes, e-learning, b-learning, support systems…), the choice of these solutions requires of a systematic approach and must be linked to some mechanisms that allow the incorporation of the most common methodological standards. These mechanisms must also follow the guidelines established by the governing bodies of the organization, thus there is a need of order, leadership and alignment of the creation of the different IT products and services related to the business processes of the university.

University Jaume I has, in this aspect, some peculiarities that have conditioned the model under development. Its recent creation (1991) and the internal structure, very centralized, have driven to the development of an ERP (that covers the 95% of the organizational procedures) that is integrated with the rest of the necessary tools for the educational organization. This fact has made that it is considered, in practice, as one of the most relevant strategic assets for the University. Given the dependency created between the business objectives (teaching, research, administration...) and the academic ERP, governing bodies of the institution are especially concerned about the availability and reliability of the IT infrastructure and the integrity and privacy of the data that it contains. For this reason, the strategic approach to IT Governance has taken as its main reference points two aspects of IT management: security aspects and software life-cycle. The description of this approach is the main objective of the present paper.

2. Background

During 2002, before formal standards for IT Governance spread, the University developed a model for the IT/IS process that included the necessary support structures. It was named "University TI/IS Framework" and it has since then evolved as a valuable IT Governance instrument for the institution, becoming part of the set of instruments that currently manages the totality of business aspects of the university and that have recently been awarded with the EFQM +500 qualification.

The main objective of the IT/IS framework is to provide the mechanisms for the incorporation of the IT based solutions at university. IT improvement must not be considered only from a technical perspective. The implantation of the ICT, commonly requires the adaptation to a set of rules and to develop new reference environments that allow to maintain or increase the guarantees of the new processes over those managed in a traditional way. It is essential that the organization apply rules, standards and methodologies that allow a safe but agile change process.

3. IT Governance at Universitat Jaume I.

Technology management at the University must be comparable against a general IT Governance reference framework, leading to the general objective of redesigning the software development work environment. In our particular case, we can measure and compare the improvements against the average results of Spanish universities using the annual UNIVERSITIC report elaborated by a workgroup of analysis, planning and IT Governance of the CRUE-TIC that is lead by University Jaume I. Currently, a revision process has been initiated using ISO/IEC 38500:2008 "Corporate Governance of Information Technology" standard as a basis for the assessment of the previous IT Governance scheme.

The ISO 27001 standard provides a formal model for "establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System". Its adoption in a university is a strategic decision involving, at some extent, the whole academic community, but specifically, the development teams. In this paper, we will show the mapping between the key aspects of ISO 38500, the control objectives of the ISO 27002 and key aspects of software life-cycles. An ISMS, also establishes a set of mechanisms that allow the organization to control and measure the correct application of the control objectives. Some important ones, which have been already applied at Universitat Jaume I, are the internal audits that together with IT indicators, continuous improvement and yearly security objectives provide the appropriate feedback mechanisms to the governing bodies.

4. References

Wikipedia. ISO 27000 series. Retrieved February 28, 2011, from: http://en.wikipedia.org/wiki/ISO/IEC_27000-series

ISO/IEC 27001:2005. Information Security Management Systems. Retrieved February 28, 2011, from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

ISO/IEC 38500:2008. Corporate Governance of Information Technology. Retrieved February 28, 2011, from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=51639.