Filling the gap of Information Security Management inside ITIL®: proposals for posgraduate students

Elena Ruiz Larrocha and Jesús M. Minguet
Software Engineering and Informatics Systems Department
UNED - Spanish University for Distance Education
Madrid, Spain
elena@issi.uned.es, jminguet@issi.uned.es

Gabriel Díaz, Manuel Castro and Alfonso Vara
Electrical and Computer Department
UNED - Spanish University for Distance Education
Madrid, Spain
gdiaz@ieec.uned.es, mcastro@ieec.uned.es,
avara@ieec.uned.es

***Abstract*—This paper describes different proposals made at UNED, for post-graduated students, at the area of IT Services Management and specially trying to fill the gap, of paramount importance, of the treatment due in ITIL® (Information Technology Infrastructure Library) to Information Security Management. We analyze the treatment given to Information Security Management in ITIL, both versions 2 and 3, and describe the different at distance post-graduated courses we offer that fill these methodologies and discuss the opinions and evaluations of our students.**

Keyword: Information security management, ITIL, ISO 27001, Professional education.

I. INTRODUCTION

Every kind of organization is increasingly dependent of IT services to satisfy their corporative objectives and to cover their business needs [1] [2] [3]. This tendency provokes that IT (Information Technologies) Service Management is becoming an important factor for the success or failure of business in many organizations. A cause of the increase costs of IT services and low quality services is due to inadequate IT Services Management or does not work of desirable form [1].

But first of all, what is Service Management? Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services. And, what is a Service? Service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

There are a number of widely applied standards and methodologies used for the alignment of Information Technologies (IT) departments with the business, inside each organization. One of the most relevant is called ITIL® (Information Technology Infrastructure Library) [4]. ITIL is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally.

After this introduction of the context where we have done our research, the rest of the paper is organized as follows.

First, we do a small introduction to ITIL (Information Technology Infrastructure Library) both versions (2 and 3) and ISO 20000. In the next section we present the Security Management basis needed and its relation with ITIL. After that, this paper describes different proposals made at Electrical and Computer Department from UNED (Spanish University for Distance Education) [5], for post-graduated students, at the area of IT Services Management. Specially we try to fill this knowledge gap, of paramount importance, of security treatment due in ITIL. We explain the characteristics of these topics at distance courses, and how we try to stimulate the acquisition of practical knowledge by the students, promoting the practical work as a significant part of their works for the course.

Finally, we show the students evaluation of the last three years for these two courses that really encourages us to refine the courses and follow in the same direction.

II. ITIL® VERSION 2

ITIL (Information Technology Infrastructure Library), nowadays the most widely accepted IT service management framework in the world. ITIL arose in the '80s developed by the Office of Commerce of the British Government (Office of Government Commerce - OGC UK), [2] [3]. It provides a set of best practices detailed description, grouped in books, offering an extensive list of roles, threats, procedures and responsibilities that can be adapted to almost any kind of IT organization. The enormous amount of topics that those publications cover makes ITIL a reference, more essential day by day, to establish new improvement goals inside an IT organization.

ITIL Version 2 (which appeared at the end of the '90s) has two big modules as you can see in Fig. 1: Service Support and Service Delivery.

The other four ITIL version 2 core books (Planning to Implement Service Management, The Business Perspective, ICT Infrastructure Management and Application Management) are out of our research, because they do not have processes so they have not the same importance than Service Support and Service Delivery have.

978-1-4244-6571-2/10/$26.00 ©2010 IEEE

Fig.1. ITIL version 2 core books (OGC source).

Inside Service Support book we can find the following six parts (which are five processes and a function): Incident Management, Problem Management, Configuration Management, Change Management, Release Management and a very important function: Service Desk.

Inside Service Delivery we can find also six parts (which are processes too): Service Level Management, IT Financial Management for IT Service, Capability Management, Availability Management, IT Service Continuity Management and Security Management.

ITIL processes all together are shown in Fig. 2, on the right you can see Service Support processes and on the left you can see Service Delivery ones:

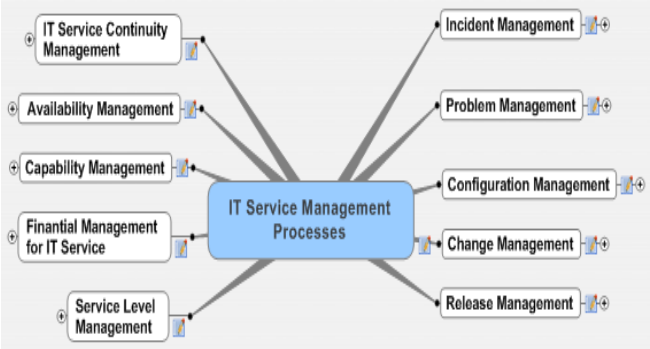

Fig.2. IT Service Management Processes (own source)

Service Support area describes how customers can access the appropriate services in order to assist to their business. Service Delivery area describes the services offered to the customer and what is required to provide those services.

III. ITIL® Version 3

Many public and private organizations worldwide implement these best practices following the version 2 of ITIL but since two years ago there is a new version that it is being implemented also, but in a much slower pace.

ITIL Version 3 [6] (also known as ITIL Refresh) took off two years ago and it has some big changes related to previous version. This new version is focused on the service lifecycle.

ITIL version 2 has undergone a major refresh which is version 3. Version 3 represents an important evolutionary step in its life. The refresh has transformed the guidance from providing a great service to being the most innovative and best in class. At the same time, the interface between old and new approaches is seamless so that users do not have to reinvent the wheel when adopting it. Version 3 allows users to build on the successes of version 2 but take IT service management even further.

Now there are only five core publications which describe the key principles of IT service management and provide a high-level overview (Service Design, Service Operation, Service Strategy, Service Transition and Continual Service Improvement).

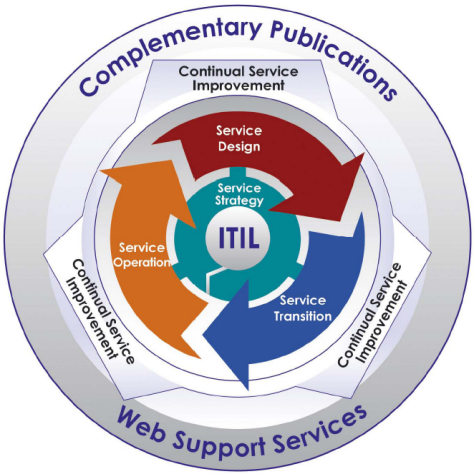

Fig.3. ITIL version 3 core books (OGC source).

IV. ISO 20000

On the other hand, on 15th December 2005 ISO (International Standard Organization) [7] adapted BS 15000 British norm (based on ITIL and developed to officially define effective service delivery requirements for the business and their clients) into a new international standard: ISO/IEC 20000.

Although ISO 20000 does not formally include ITIL exposition, it does describe a set of management processes aligned and complementary to what ITIL defines.

ITIL provides guidance on what should be done in order to offer users adequate IT Services to support their business processes. ITIL certifications are available for individuals but until recently there was no way for an IT organization to prove that it is working along the ITIL recommendations. The ISO 20000 standard was conceived to fill this gap. Initiated by the two organizations itSMF (IT Service

Management Forum) [8] and BSI (British Standard Institute), it is modeled upon the principles of ITIL and for the first time offers IT organizations the possibility to have their IT Service Management certified.

Actually it is considered that each ITIL book offers deeper information and a best practices guide about subjects located in the scope of ISO 20000 norm. In contrast to the ITIL books, ISO 20000 does not offer specific advice on how to design your processes. It is rather a set of requirements which must be met in order to qualify for ISO 20000 certification.

The great implantation on private and public sector companies and the need of organizations to demonstrate their work this way by means of ISO 20000 certification, is causing a great demand of professionals on this field.

V. SECURITY MANAGEMENT

Information Security describes activities that relate to the protection of information and information infrastructure assets against the risks of loss, misuse, disclosure or damage. Information Security Management (ISM) describes controls that an organization needs to implement to ensure that it is sensibly managing these risks.

The risks to these assets can be calculated by analysis of the following issues:

- Threats to your assets. These are unwanted events that could cause the deliberate or accidental loss, damage or misuse of the assets.

- Vulnerabilities. How susceptible your assets are to attack.

- Impact. Is the magnitude of the potential loss or the seriousness of an event.

Standards that are available to assist organizations implement the appropriate programmes and controls to mitigate these risks are for example ISO 27001, ITIL and COBIT.

We consider that ISM has crucial importance because almost every company (even smallest ones) does their job using networks into their organization to exchange internal information, and uses Internet too. Each day is more necessary to deal with possible security problems on a global way, considering external threats from Internet but also internal treats. Information Security aspects are really important for company success and business stability.

VI. ITIL AND SECURITY MANAGEMENT

It is a proven fact that ITIL version 2 has a great weakness on Security matters. Between the existing set of Service Delivery books, there is a small one, called Security Management, that shows on a very light way what to do with security, and there is no later reference about this point in any other book of this version. Because of this weakness, organizations that implemented ITIL version 2 since years ago have had to fill this gap by their one, using other kind of approaches. That is the reason why Security Management process does not even appear in Fig. 1.

Nevertheless, on ITIL version 3, concretely in Service Design book, we can find much more information about what to do with Security Management. Although this new version touches Security on a deeper way, there are lots of links in the mentioned book to ISO 27001, which is the world wide extended standard followed on security subject.

Therefore, ITIL version 3 gives a much adequate treatment [9] to security that ITIL version 2 does, identifying the details of the structure and implementation of the Information Security Management process with the good practices for implementing an ISM System (ISMS) included in the ISO 2700x family of standards.

ISM needs to be considered within the overall corporate governance framework. Corporate governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that the objectives are achieved, ascertaining that the risks are being managed appropriately, and verifying that the enterprise resources are used effectively.

The purpose of the ISM process is to align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities.

An information security management system (ISMS) is, as the name implies, a set of policies concerned with information security management. The idiom arises primarily out of ISO/IEC 27001.

The key concept of ISMS is for an organization to design, implement and maintain a coherent suite of processes and systems for effectively managing information accessibility, thus ensuring the confidentiality, integrity and availability of information assets and minimizing information security risks.

As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. ISO/IEC 27001 therefore this incorporates the typical "Plan-Do-Check-Act" (PDCA) Deming approach to continuous improvement:

- The Plan phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.

- The Do phase involves implementing and operating the controls.

- The Check phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.

- In the Act phase, changes are made where necessary to bring the ISMS back to peak performance.

The best known ISMS is described in ISO/IEC 27001 and ISO/IEC 27002 and related standards published jointly by ISO and IEC.

Another competing ISMS is Information Security Forum Standard of Good Practice (SOGP) [10]. It is more best practice-based as it comes from ISF's industry experiences.

VII. The Computing Engineering Students Problem

On the other hand, Spanish students on Computing Engineering, when they finish their degrees, have little or no idea on Security Management and surely no idea at all about ITIL. If we are talking about the huge importance of ITIL all over the world, as the most accepted approach to IT service management, how is this possible?

We face a situation in which students that finish the Computing Engineering careers, at least in Spain, don't know all these kind of standards and methodologies and don't have a practical, day to day, approach to implement and maintain a good information security policy within an organization.

It is well known that the alignment of Information Technologies (IT) departments with the business is essential, and ITIL best practices are probably the best solution. That is the reason why from UNED we are trying to fill this gap in students knowledge, because at the moment we really believe this is a weakness. So, we are teaching post-graduated students to be experts on these topics, both Security Management and ITIL, just to be ready for the real world.

VIII. The UNED Solution

As everybody knows, UNED has distance students almost all over the world, so the way we teach is a little peculiar. We normally never met our students, therefore, teacher-student communication has everything to do with new technologies platforms, Internet and so on.

Our guidance and attention to students is made using computing and telecommunications, utilizing email on Internet or Learning Management Systems and, when this kind of communication is not possible, we attend them by telephone, post mail or fax.

Our attention is personalized, proper of a high quality education, which is a feature common in all UNED actions. Most part of material is given to students at the beginning of the course, so they can plan their study rhythm. Sometimes, when necessary, we make presence sessions using videoconference.

In addition to all this, during the courses we propose students to do a end of course personal work, that we correct, inform and send back to them, so they are able to evaluate themselves and improve their knowledge.

Due to all the reasons explained before, and trying to take advantage of the professional practice of some of the authors, from Electrical and Computer Department, four years ago we began to offer post-graduate at distance courses for helping students to understand all these matters.

At the moment we offer [11] two related courses:

1- Professional Expert in IT Services Management based on ITIL® and ISO/IEC 20000.

2- Professional Expert in Information Security for Computer Networks.

Professional Expert in IT Services Management based on ITIL® and ISO/IEC 20000 main goal is giving enough knowledge to students, so they can use a common language in service management based on ITIL. Also they get a very high level to face up ITIL foundations examination certification (1 hour multiple choice exam: basic understanding of the ten ITIL Service Delivery and Service Support processes and the Service Desk function).

Besides this, we try students understand tight relationship between ITIL and ISO 20000 and also students know different approach for new ITIL version 3. Each course is divided in four parts: introduction, 2 didactic units and the student's final work. The didactic units of this course (with three chapters in each unit) are the following:

1- IT Service Management and its implementation using ITIL best practices.
   a. Introduction to IT Service Management.
   b. Service Support Processes.
   c. Service Delivery Processes.

2- UNE/ISO 20000 standard and ITIL new version.
   a. ISO 20000 analysis and description.
   b. Life cycle new approach on ITIL version 3.
   c. Implementing ITIL version 3 practices.

Professional Expert in Information Security for Computer Networks main goal is giving to student completely updated technical knowledge on systems security and communications networks of computers. This course has two units (with three chapters in each unit):

1- Infrastructure security, systems security, organization security and biometrical systems.

a. Information Security at networks computer. Protocols at client/server communications.

b. Security Policy for company networks. Security attacks at network company classification.

c. Use of biometric techniques in security.

2- Cryptography and defense to attacks of security networks.

a. Introduction to Cryptography.

b. Modern Cryptography. Public and private keys Cryptosystems.

c. Non cryptographic defenses and cryptographic defenses at communication networks.

In our Information Security course first unit we also describe the goal and scope of Spanish laws which determine how to face the security problem of personal data files protection (LOPD, Spanish Law for Data Protection) [12] and also we describe security conditions on web servers (LSSICE, Spanish Law for Service Information Society and Electronic Commerce) [13]. More than 90% of our computer network traffic are TCP/IP [14] messages, so our students also study the comparison between stack IP and standard architecture OSI (Open Systems Interconnect) [15].

IX. Data and Tests Results

To keep in touch with the students real needs, we always make some exhaustive tests to our post-graduated students, to analyze if we are going in the right direction. And the results make us stand by.

As an example, these are some few questions and answers obtained during the last years:

1. To the question: Did you receive additional information about contents of your interest related with the course? Students respond yes: 91%.
2. To the question: Were your expectations about the course satisfied? Students respond yes: 86%.
3. To the question: Could you access to experts demonstration about application questions of the course? Students respond yes: 83%.
4. To the question: How do you value the course? Students respond yes: 86%.
5. To the question: Will you register in any other similar course? Students respond yes: 94%.
6. And finally, to the question: Will you recommend this course to anyone? Students respond yes: 92%.

In general, students' opinions should be very important at any university, but especially for us (teachers from UNED). We must know their opinions, checking that kind of feedback information, to be continually improving our methods and techniques to teach.

As we have explained above, we evaluate students with two kinds of tests. Firstly we evaluate them with at distance assessments for each unit that we correct and then we send the results and comments necessary to make students improve. And finally we evaluate students with a personal final work, which requirements are published at our web server. We are very proud of most of them. Examples of those final works are the following tittles:

- "Assessment of commercial and open source solutions for implementing Configuration Management Data Bases (CMDB): HP, Symantec, OneCMDB and ControlTier solutions"
- "Implementation of ITIL-based good practices to audio and video services"
- "ITIL and Prince2: Services Management and Projects Management"

This new academic year we are going also to give a new step in the ITIL course, trying to help the students to prepare the ITIL Foundations Certificate exam by having mobile evaluation tests on the main ITIL concepts. It will be as part of a European project, called mPSS (mobile Performance Support System for Vocational Education and Training).The students will have a number of simple tests, based on the ideas of well proven [15] DIPSEIL project for individualized high performance e-learning system, accessible from Internet via mobile devices, specifically mobile phones. The main idea is that the students can assess their knowledge of the main concepts related to ITIL and ISO 20000 at every moment and from anywhere and it will be part of several pilots related with the same high performance and individualized methodology, used also for another European Project, IPLECS (Internet-based Performance-centered Learning Environment for Curricula Support) that tries to build a complete European Engineering Master, completely accessible via mobile devices and for every European student.

X. Conclusions

In this paper we begin discussing what we think is a need to explain the differences in the approaches, of both versions of ITIL, to Information Security and the need for the graduate students to know, at least at a foundation level, these best practices approaches and standards.

With those two proposals from UNED, concretely from Electrical and Computer Department, we are trying to fill the gap we have just presented in this paper. We consider it is absolutely necessary students know all this

methodologies, standards, laws ands concepts before they start working at any company in Spain or anywhere in the world.

Analyzing the results of the students' tests done at the end of each of our post-graduated courses, we conclude this is the path we have to follow to align students' knowledge and real world needs.

ACKNOWLEDGEMENTS

The authors would like to acknowledge to the European Union Socrates the support in the IPLECS Project – Internet-based Performance-centered Learning Environment for Curricula Support Project ERASMUS 141944-LLP-2008-1-ES-ERASMUS-ECDSP as well as in the Project 142788-2008-BG-LEONARDO-LMP mPSS – mobile Performance Support for Vocational Education and Training Project.

REFERENCES

[1] E. Ruiz, "Una Propuesta Organizativa de los Procesos SD y SS en ITIL", Revista Española de Innovación, Calidad e Ingeniería del Software (REICIS), Vol.3, No 2, 2007. Accesed November 2009. http://www.ca.com/hk/event/itil2005/bjohnson.htm.

[2] Office of Government Commerce (OGC), ITIL Managing IT Service: Service Delivery, TSO, London, 2001.

[3] Office of Government Commerce (OGC), ITIL Managing IT Service: Service Support, TSO, London, 2001.

[4] Official ITIL® Website, accesed August 2009. http://www.itil-officialsite.com/home/home.asp

[5] UNED Official Website, accesed November 2009. http://portal.uned.es/portal/

[6] ITIL v3. Official ITIL® Website, accesed November 2009. http://www.itil-officialsite.com/home/home.asp

[7] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements , accesed August2009. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[8] itSMF Official Web Site, accesed November 2009. http://www.itsmfi.org/ and its Spanish Official Web Site, accesed November 2009. http://www.itsmf.es/

[9] J. Clinch, OGC, "ITIL V3 and Information Security", accesed August 2009. http://www.best-management-practice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf

[10] Information Security Forum Standard of Good Practice (SOGP) fficial Website, accesed November 2009. https://www.isfsecuritystandard.com/SOGP07/index.htm

[11] Programa de cursos de Tecnologías de la Información y Comunicaciones, accesed August 2009. http://volta.ieec.uned.es/programa_TIC.asp http://www.itil-officialsite.com/home/home.asp

[12] LOPD Official Web Site, Ley Orgánica de Protección de Datos, accesed November 2009. https://www.agpd.es/portalweb/index-ides-idphp.php

[13] LSSICE Official Web Site, Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, accesed November 2009. http://www.lssi.es/

[14] TCP/IP Official Web Site, accesed November 2009. http://es.wikipedia.org/wiki/TCP

[15] OSI Official Web Site, accesed November 2009. http://es.wikipedia.org/wiki/Modelo_OSI

[16] G. Díaz, M. Castro, E. López, S. Martín, E. Sancristobal, J. Peire, C. Martínez y N. Mileva, "New individualizad Task-oriented professional e-Learning courses", eChallenges e-2007 Conference, The Hague (Netherlands), October 2007, in P.&M. Cunninghan (Eds): "Exploiting the Knowledge Economy: Issues. Application and Cases Studies", IOS Press Ámsterdam, ISBN 978-1-58603-801-4, 2007