UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática,* <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Pro Dialog, journal from the Polish CEPIS society PTI-PIPS

Cover page designed by Concha Arias Pérez
"Strategos" / © ATI 2008
Layout Design: François Louis Nicolet
Composition: Jorge Llácer-Gil de Ramales

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (April 2008)

"Model-Driven Software Development"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. IX, issue No. 1, February 2008

Monograph: IT Governance (published jointly with Novática*)

Guest Editors: *Dídac López-Viñas, Antonio Valle-Salas, Aleix Palau-Escursell, and Willem-Joep Spauwen*

UPENET (UPGRADE European NETwork)

CEPIS NEWS

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

Implementing IT Governance Ad@pting CobiT, ITIL and Val IT: A Respectful Caricature

Ricardo Bría-Menéndez and Manuel Palao García-Suelto

In this article we present some guidelines for the combined use of three reference models and a series of points and criteria to be considered in respect of their complementarity.

Keywords: CobiT, Governance, IT Governance, ITIL, Val IT.

1. It is our intention to respond to UPgrade's kind invitation to write "an article explaining how to put to work, on a joint basis, CobiT and VAL IT, and maybe ITIL".

2. The title chosen addresses the invitation, highlights the objective (Implementing Good IT Governance), and introduces a neologism, ad@pting, as a healthy mix of adopting and adapting. We hope the article will honour the title and explain, if not justify, our ad@ption of the neologism.

3. Good IT Governance is a topic of utmost importance, one which is getting hotter by the day and has increasing but still lagging interest for businesses, professionals, consultants, and society as a whole.

4. It should concern society, as ICT's pervasiveness is ever expanding in enterprises, institutions, and society and because in Good Corporate or IT Governance we all have a voice (or will end up having one)[1].

5. It has been said that the adequate restatement of an issue is more than halfway to solving it. It is the purpose of the authors to help our readers with an honest and modest attempt at restatement.

6. The usual length limitation set for this article but, above all, the intrinsic communicational limitations of the authors may lead the reader to a hasty impression that the whole subject is just a matter of grandiose caricature statements, when the authors (from their professional training, experience and principles) know and preach the opposite: the subtleties, the greys, and the maybes.

7. As a first example of "caricature statement": we do not believe that CobiT, Val IT or ITIL can be implemented in organizations.

Authors

Ricardo Bría-Menéndez has specialized in the areas of consulting and auditing and, for the last 10 years, in the emerging topic of IT Governance, which he puts as a top priority in the agenda of enterprises and organizations across the world. Since 1982, he has been an active member of ISACA *(Information Systems Audit and Control Association*). ISACA is a professional organization recognized as a world leader in Governance, Assurance and Security where Ricardo has sat on numerous boards and committees, and was elected as International Vice President. Mr. Bría's professional career has been developed in the United States, Latin America and Europe. For many years he worked for a large international auditing and consulting firm and was also Organization and Process Improvement Manager for a major international Bank. He is CISA (*Certified Information Systems Auditor*) and ACT (*Accredited CobiT Trainer*) certified by ISACA, and graduated in Business Administration at the University of Texas at Dallas <rbria@safecg.com>.

Manuel Palao García-Suelto holds an ABD in Computer Sciences and Civil Engineering and has Bachelor Degrees in Statistics and Operations Research, and Sociology. He is CISA (*Certified Information Systems Auditor*), CISM (*Certified Information Security Manager*) and ACT (*Accredited CobiT Trainer*) certified. He has been an ATI (the Spanish Association of Computer Technicians) Senior Member since 1975 and Co-coordinator of Novática's (the journal of ATI) Technical Section "IT Audit" for the past six years. He has been Managing Partner of *Personas & Técnicas: Soluciones, SLU*, and Partner and CTO of *The Model Company, Modelco SL*. He served as President of ISACA's Madrid Chapter for two terms. Professor at UCLM's Master Program on IT Security and UPM+ALI's Master Program on IT Security and Audit; Professor and Area Coordinator at Deusto University's Master Program on IT Governance. He has authored a book on MIS, and has also written several chapters for books and more than 200 articles <mpalao@personasytecnicas.com>.

8. This "non-implementability" requires a prior reflection on regarding frameworks (such as CobiT, Val IT and ITIL), their needs, characteristics, and differences with many other standards. This exercise of reflection is much needed and of considerable importance as there appears to be considerable confusion (fuelled by some spurious interests) regarding standards and frameworks and their certifiability, compatibility and profitability.

[1] Good IT Governance is meant to serve stakeholders' interests. The AS/NZS 4360:2004 *Risk Management* standard defines stakeholders as those *"who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk."*

9. The following characteristics are being proposed in general, tentative terms as we are unaware of a more rigorous taxonomy or definitions. Frameworks, generally, are oriented towards "best practices", while standards are oriented towards "minimum requisites". Frameworks deal more with "what" and standards with "how". Frameworks have a broader scope, are more flexible and compatible; standards are more stringent, rigid and self-contained, when they are not actually exclusive.

10. Good frameworks are needed to ensure, in the broadest possible way, that IT resources are aligned with the business/service objectives of the enterprise/institution, and that services rendered and information provided comply with the minimum requirements of quality (cost, distribution, quality), security (confidentiality, integrity, availability) and trust. They are a code of good (or best) practices.

11. According to COSO[2], which we familiarly call "the Mother of all Control Frameworks", fiduciary or trust-related requirements are intended to ensure the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with laws and regulations.

12. In our global and highly interrelated world, there must be and there must be seen to be significant convergence between the various efforts to produce and maintain frameworks and standards. If such convergence does not happen or if it is not seen to be happening at a reasonable speed, one may suspect the existence of hidden interests and artificial barriers which (as a result of being driven by hidden agendas) may pose serious risks for those not sufficiently well informed.

13. This same general convergence can be seen in the history of art (romanticism in music, cubism in painting) and - due to its particular nature - in the history of science (Boyle-Mariotte in the XVII century, with their 'ideal gas'; Watson-Venter, the day before yesterday, with the human genome; or the counterexample in Spain in the mid-20th century, under Franco's dictatorship, when Professor Julio Palacios maintained, in front of important audiences, the radical falseness of Einstein's Theory of Relativity[3]. This latter example of divergence is not trivial. Sadly, unscrupulous visionaries and liars often speak louder than those who, by trial and error, seek the right path.

14. A similar trend towards convergence can be seen in the specific case of the frameworks and standards that interest us. Here are a couple, by way of example:

15. One: ISO 9001:2000 (as opposed to ISO 9000:1996) introduces and highlights the consideration of "customer satisfaction" in convergence, for example, with EFQM (introduced in 1992), in turn converging with the US "*Malcolm Baldrige National Quality Improvement Act"* of 1987 (100-107).

16. Another: ITIL (a product created in 1986 by the UK Government (CCTA) for the UK Government) in 1991 decided to try and expand its approach to private enterprise, in convergence with ISACA's Control Objectives (1976), the forerunner of CobiT (1996).

17. Where the general convergence of standards and frameworks stands out is in their preference for improvement process over the milestone. In this respect, probably the most widely known reference is Deming's PDCA wheel: Plan-Do-Check-Act.

18. A good framework, according to generally accepted principles, must meet the following four requirements:

19. First of all: process orientation. This basically means that all activities are organized into processes (that are more or less repeatable, documented and traceable, among other properties described by most 'maturity models') which have a "process owner" with clearly defined responsibilities. For the purpose of this article, the focus is on good IT Governance, as a means of meeting business needs while narrowing the gap between risks and control requirements and helping to optimize IT-related investments by providing the means for measuring and evaluating them.

20. Secondly, it has to be based on commonly accepted practices such as technical standards (ISO, EDIFACT, etc), codes of ethics (Council of Europe, OECD, ISACA, etc.), systems, and IT process qualification criteria (ITSEC, TCSEC, ISO9000, SPICE, TickIT, Common Criteria, etc.), internal audit and control professional standards (COSO, CICA, IFAC, IIA, AICPA, GAO, PCIE, ISACA, etc.), industry and governmental requirements and practices (ESF, IBAG, NIST, DTI, BS7799, etc.).

21. Thirdly, common language. The use of common terms (provided by a framework) enables and encourages communication between members at different levels and in different departments of the enterprise, and with consultants, customers, vendors, and third parties in general, while avoiding misunderstandings resulting from different – even opposite - interpretations of the same word. It also helps to bridge the traditional communications gap between business and technology and to establish objective, intelligible, and shared metrics and indicators.

22. Lastly, good frameworks take into account the promotion and adoption of regulatory requirements. Regulatory compliance is a complex and costly task. The adoption

[2] Copyright © 1985-2006 The Committee of Sponsoring Organizations of the Treadway Commission.

[3] Thomas F. Glick: "*Ciencia, política y discurso civil en la España de Alfonso XIII*". *Espacio, Tiempo y Forma, Serie V, f-i." Contemporánea*, t. 6, 1993, pp. 81. <http://62.204.194.45:8080/fedora/get/bibliuned:ETFSerie5-657A3C0B-A3E9-D95C-E289-6D65020EC50E/PDF>.

of a framework based on generally accepted standards facilitates compliance and helps demonstrate compliance to third parties.

23. Good frameworks are not radical or fundamentalist; rather, they are tolerant. They facilitate and even promote a cooperative promiscuity between different standards and frameworks. It is a shame though, that some people, out of ignorance or vested interest, try to misuse a good framework!

24. An outstanding example of positive framework hybridization is provided by ISO "management systems" (considered here as a single framework). ISO 9001:2000 (Quality Management), ISO 14000:2004 (Environmental Management), and ISO 27001:2005 (Information Security Management). Three standards on quite different subjects, sharing a common framework (the "management system"). In the recent words of a prominent AENOR (Spanish Association for Standardization and Certification, the Spanish member of ISO) executive: "the same engine [or framework, to use our word] with different data". The three standards (and others that will presumably be joining them soon) share structure, documentation and procedures, which enables, simplifies and increases the benefit of their everyday joint use (not just their joint certification or re-certification).

25. But the most paradigmatic example in our area of concern is perhaps CobiT mapping to other frameworks and standards. To date (December, 2007) ISACA, in addition to its general mapping to "good international practices", has published 9 CobiT maps to specific frameworks or standards (CMMI for Development, ISO/IEC 17799:2000, ISO/IES 17799:2005, ITIL, NIST SP800-53, PMBOK, PRINCE2, SEI's CMM for Software, TOGAF 8.1). We also know that CobiT mapping with ISC2 CBK, the framework underlying CISSP, is currently in the pipeline.

26. In addition to all the above, good frameworks are democratizing. We use the term here to mean that their features make them applicable (ad@ptable) to any organization, regardless of industry and/or size, due to the fact that good frameworks consider the whole picture in a holistic manner, but divided into manageable and independent, albeit interrelated, parts with well-defined and responsible limits and relationships, and with a clear and precise assignment of rights and obligations.

27. Successfully ad@pting a good framework (or a number of them as they are not mutually exclusive), also have a "revolutionary" and distinguishing quality: small/immature organizations can take a leap forward and position themselves in the best-of-breed category (where one would normally only expect to see Fortune™ 1000 companies). This (fortunately, since it represents a window of opportunity) clashes with the rigid ideology of 'maturity models' interested in selling a supposedly inexorable "phase by phase" (or fascist goose stepping) approach.

28. Going back to where we were a few paragraphs ago, we claim that CobiT, ITIL or Val IT cannot be implemented in the sense of implanted *"to fix or set securely or deeply*[4]", as in the case of a pine tree in the backyard, a dovetail joint in the carpenter's shop, or a kidney in the operating theatre. Those are events or, to be more precise, they are the final concrete, permanent and tangible outcome of a project.

29. Frameworks are "adopted" and "adapted" (ad@pted) in a living and continuous process in which an enterprise/institution, starting from any stage, sets sail towards ever higher levels of excellence (the journey being more important than the destination).

30. To arrive at the destination it is of utmost importance to choose the right vehicle for the journey. However, apart from selecting which framework or frameworks (since nobody today is at risk of dying from a lack of frameworks, standards and best practices), maybe the most critical success factor for the trip is who makes the decision and who sponsors the journey.

31. This is a process that cannot flow upstream, against gravity.

32. If the project is driven and sponsored by Top Management (TM), its success is not totally guaranteed beforehand.

33. But its failure is assured if that condition is lacking.

34. The factotum then must be (note the imperative form) TM, an issue which is often ignored (more or less blatantly). The main reason being that, among its responsibilities for corporate governance, it also has a responsibility for IT governance and an obligation to, implicitly or explicitly, select the components and choose the framework "cocktail" of its liking.

35. One cannot but hope that in the not so distant future, in a more informed and cultured arena, the current could, as it does in estuaries, allow the passage of certain amount of upstream traffic, i.e., well founded and documented suggestions taken up to the Top Management (TM) by second/third line management or staff personnel. But, while such a sensibility/culture does not become generalized (thanks mainly to professional associations, universities, consultants, etc.), all the power and potential for success lies with the TM.

36. The "implementation"/ad@ption is then a process (an endless one!; Deming's virtuous circle). A process of par-

[4] Merry Webster Dictionary <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=implanted >.

tial ad@ption, of cutting, pasting and ad@pting what suits us; a process of hybridization or crossbreeding.

37. As previously stated, good frameworks are not radical. Quite the contrary, they are tolerant: they accept and even foster promiscuity, cutting and pasting while remaining faithful to their essence and remaining compatible with other good frameworks, which is another of their intrinsic characteristics. In a way, it is like medieval Toledo where frameworks as different as the ones introduced by the Jewish, the Christians, and the Arabs caused culture and prosperity to flourish in synergy.

38. Another "caricature statement" deals not with the what but with the how.

39. As frustrating as it might seem for most consulting firms (and even more for their major clients) whose business model is to sell many "junior" and inexperienced hours (pyramidal model) instead of fewer "senior" expert hours of consultancy (not just PR), the critical issue here is not the product (e.g., the ITIL version), or the what. Rather it is the how, the process; the project; how it is managed, how and how rapidly it is expanding, who is involved and who is committed (remember the fable of the pig and the hen, and their attitude in the face of the consequences for each of them of not providing us with ham and eggs).

40. A good simile to describe the 'how' could be that of cultivating, agriculture and culture (same etymology). Good Governance is not about implementation but about cultivating, about work through the generations, about a continuous and sustainable process, relying more on the essentials and on workmanship than on fashion.

41. Sustainability also assumes a number of prerequisites that are so self-evident and naive that it seems absurd to mention them. But we have to mention them due to the numerous and widely documented blunders made by important corporations, assisted by major consulting firms, while attempting to ensure that projects designed to meet the requirements of the Sarbanes-Oxley Act delivered sustainable structures and procedures.

42. Good IT Governance cannot be a patch or an orthopaedic limb. It has to be rooted in the organization's most important, genuine, and healthy fibres.

43. Paraphrasing the famous quote by Lord Kelvin "If you cannot measure it, you cannot improve it", we would like to introduce another of our own "What is not continuously evaluated and improved becomes obsolete before leaving the drawing board".

44. Having mentioned more than once promiscuity and tolerance, it might seem that frameworks and standards do not ultimately contribute anything - that they are unnecessary or mere divertissement. A hasty and mistaken conclusion! Frameworks are not only necessary, but are a mandatory prerequisite to pave the way towards good IT governance.

45. Frameworks are the crystallization of a "body of knowledge" and "guidelines" that summarize the hands-on experience of hundreds of international and multi-industry IT practitioners in working groups and committees of professional organizations and associations. The end result of their contributions is objectively overwhelming, particularly for those who, in this day and age, may still be trying to reinvent the wheel.

46. Fortunately, thousands of the best professionals, from many different areas, countries, and cultures have put in their time as volunteers and helped to develop and keep CobiT (Control Objectives for Information and related Technologies) current. CobiT has already become the internationally accepted reference IT Governance framework, refining practices that have proved successful after numerous implementation cycles.

47. The fact that frameworks are not intended to/cannot be applied by themselves as a master recipe should not mislead us into undervaluing them, but rather the opposite. Competitive and surviving organizations stopped thinking that the isolated self-sustaining Robinson Crusoe approach was the way to go a long time ago

48. In Forrester's opinion, "first use CobiT for IT control and governance, ITIL for service delivery and support, and finally use ISO 17799 for Security" [5].

49. To which, humbly, in view of the authority of the quoted sentence, we dare add, as a cherry on top of the cream: "Use Val IT to realize the benefits and the value generated by the process".

50. By way of a conclusion: if you seriously want to implement good IT governance in your company/institution, just do it, using your own customized recipe, ad@pting CobiT, ITIL, and Val IT. If you feel like it, drop a green olive into the bowl.

51. If you do it right, you'll be embarking on an endless process (just like all successful projects).

52. If you see fit to request assistance from a consulting firm, make sure they do not offer/deliver 'snake oil'. The more product-related or radical/exclusive the proposed solution is, the more suspicious you should be.

[5] January 5, 2006,COBIT Versus Other Frameworks: A Road Map To Comprehensive IT Governance by Craig Symons.