The Proceedings of the 11th European Conference on eGovernment

Faculty of Administration,
University of Ljubljana, Ljubljana,
Slovenia
16-17 June 2011

Edited by
Maja Klun, Mitja Decman and Tina Jukić
University of Ljubljana

Papers have been doubleblind peer reviewed before final submission to the conference. Initially, paper abstracts were read and selected by the conference panel for submission as possible papers for the conference.

Many thanks to the reviewers who helped ensure the quality of the full papers.

These Conference Proceedings have been submitted to the Thomson ISI for indexing.

Further copies of this book can be purchased from http://academic-conferences.org/2-proceedings.htm

ISBN:978-1-908272-01-0 CD

Published by Academic Publishing Limited
Reading
UK
44-118-972-4148
www.academic-publishing.org

Contents

Paper Title	*Author(s)*	Page No.
Preface		vi
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		vii
Biographies of contributing authors		ix
Evaluation of eGovernment Implementation at Federal, State and Local government Levels in Malaysia	*Ahmad Bakeri Abu Bakar*	1
ICT Education and Access as Strategies to Generate and Distribute eGovernment Content	*Fatemeh Ahmadi Zeleti and Erja Mustonen-Ollila*	10
The Role of National Culture on Citizen Adoption of eGovernment websites	*Omar Al-Hujran and Mahmoud Al-dalahmeh*	17
A Framework for Transitioning to Mobile Government	*Shadi Al-khamayseh and Elaine Lawrence*	27
The Stages of eGovernment: Correlation Between Characteristics That Affect eGovernment Systems	*Madi Al-Sebie*	36
Social Media in European Governmental Communication	*Isabel Anger and Christian Kittl*	43
Technology Adoption and Innovation in Public Services: The Case of eGovernment in Italy	*Davide Arduini, Mario Denni and Gerolamo Giungat and Antonello Zanfei*	53
Pan-European eGovernment and eHealth Services in Slovenia	*Jaro Berce, Vasja Vehovar, Ana Slavec and Mirko Vintar*	65
Enhancement of Public Service Effectiveness by Partially Automating Service Request Paper Forms Using Citizen ID Smartcard	*Choompol Boonmee, Rattapol Chatchumsai, Tawa Khampachoa and Chakri Chuenurah*	74
Development of User Authentication for web Application Sign-on Mechanism Using Oasis SAML Standard With Thai Citizen ID Card	*Choompol Boonmee, Peera Tharaphant and Pipop Damtongsuk*	80
A Pilot Development of PKI Digital Signatures on Electronic Correspondence Using Citizen ID Smartcards	*Choompol Boonmee, Peera Tharaphant and Pipop Damtongsuk*	87
Development of an Electronic Correspondence Time-Stamping Service Using Oasis Digital Signature Services	*Choompol Boonmee, Rattapol Chatchumsai and Sunet Boonmee*	97
Framework Guidelines to Measure the Impact of Business Intelligence and Decision Support Methodologies in the Public Sector	*Roberto Boselli, Mirko Cesarini and Mario Mezzanzanica*	107
Avoiding Disasters – Ensuring PKI-Service Availability	*Harald Bratko, Peter Lipp and Christof Rath*	116
Achieving Optimum Balance in the Simplification of tax Compliance Obligations for Business Customers and Management of Compliance and Collection Risks by Revenue	*Leonard Burke and Kieran Gallery*	124

Paper Title	*Author(s)*	Page No.
Risk Management in a Cooperation Context	*Walter Castelnovo*	132
The Effect of User's Satisfaction of web Security on Trust in eGovernment	*Lichun Chiang, Ching-Yuan Huang and Wu-Chuan Yang*	140
A Common Process Model to Improve eService Solutions - the Municipality Case	*Marie-Therese Christiansson*	149
Measuring Performance of eGovernment to the Disabled: Theory and Practice in Taiwan	*Pin-yu Chu, Tong-yi Huang and Ning-wan Huang*	158
Predictive Analytics in the Public Sector: Using Data Mining to Assist Better Target Selection for Audit	*Duncan Cleary*	168
Citizen Participation in Urban Planning: Looking for the “E” Dimension in the EU National Systems and Policies	*Grazia Concilio and Francesco Molinari*	177
Social Media and Local Government in England: Who is Doing What?	*Martin De Saulles*	187
Electronic Health Records Management and Preservation: The Case of Slovenia	*Mitja Decman*	193
Sustaining Electronic Governance Programs in Developing Countries	*Zamira Dzhusupova, Tomasz Janowski, Adegboyega Ojo and Elsa Estevez*	203
Adapting Family Card System by Means of Smart Cards	*Magdy Elhennawy, Tarek Saad, Ashraf abdel Wahab and Sameh Bedair*	213
Collaborative Network Analysis of two eGovernment Conferences: Are we Building a Community?	*Nuša Erman and Ljupčo Todorovski*	225
E-Identity, E-Activities and E-Political Participation: How are College Students Embracing the Promise of the Internet?"	*Marcoux Faiia*	234
Semantic-Driven eGovernment: Correlating Development Phases with Semantic eGovernment Specific Ontology Models	*Jean Vincent Fonou Dombeu and Magda Huisman*	245
Towards a Unified Semantic-Driven Methodology Framework for eGovernment Systems Development	*Jean Vincent Fonou Dombeu and Magda Huisman*	254
An Information System to Collect and Analyze Data From Educational Units During Epidemy Spread Periods	*John Garofalakis, Andreas Koskeris, Evangelia Boufardea, Theofanis Michail and Flora Oikonomou*	263
Interoperability in the Justice Field: Variables That Affect Implementation	*Mila Gascó and Carlos E Jiménez*	272
eGovernment and Service Delivery at the Local Level: A Comparative Analysis of Three Canadian Municipalities	*John Grant, Frank Ohemeng and Roberto Leone*	280

Paper Title	*Author(s)*	Page No.
Crowd-sourcing Techniques: Participation, Transparency and the Factors Determining the Co-Production of Policy	*Mary Griffiths*	288
Implementation of a Contact Centre in a Swedish Municipality	*Kerstin Grundén*	296
An Outline of the Technical Requirements on Governmental Electronic Record Systems Derived from the European Legal Environment	*Bernhard Horn, Gerald Fischer, Roman Trabitsch and Thomas Grechenig*	303
Examining Influences on eGovernment Growth in the Transition Economies of Central and Eastern Europe: Evidence from Panel Data	*Princely Ifinedo*	310
Management of Latvian Government Communications During an Economic Crisis: The Role of Information Strategies in the Public Sector	*Aleksis Jarockis*	320
Business/IT Alignment as Enabler for eGovernment in Syria	*Raed Kanaan, Kamal Atieh and Omar Subhi Aldabbas*	328
Does eTaxation Reduce Taxation Compliance Costs	*Maja Klun*	335
International Assistance Relationship to eGovernment Development and Benchmarking	*Endrit Kromidha*	339
Challenges to the Design and use of Stages-of-Growth Models in eGovernment	*Devender Maheshwari, Anne Fleur van Veenstra and Marijn Janssen*	347
Developing Measures for Benchmarking the Interoperability of Public Organizations	*Devender Maheshwari, Anne Fleur van Veenstra and Marijn Janssen*	354
Barriers to Developing eGovernment Projects in Developing Countries	*Zaigham Mahmood*	363
Digital Inclusion: a target not always desirable	*Fausto Marcantoni and Alberto Polzonetti*	369
Multi-Level Interoperability for ICT-Enabled Governance: A Framework for Assessing Value Drivers and Implications for European Policies	*Gianluca Misuraca, Giuseppe Alfano and Gianluigi Viscusi*	377
Strategies for eGovernment Implementation in Developing Countries: A Case Study of The Botswana Government	*Racious Moilamashi Moatshe and Zaigham Mahmood*	386
The use of ICT by Government Departments and Parastatals in South Africa	*Matsobane Frans Mosetja*	394
The Workload for the Structural Implementation of eDemocracy: Local Government Policy Issues Combined With the Policy Cycle and Styles of Citizenship.	*Bert Mulder and Martijn Hartog*	399
Channel Shift - a UK Customer Response	*Darren Mundy, Qasim Umer, and Alastair Foster*	406

Paper Title	*Author(s)*	Page No.
eGovernment in Social and Economic Development: The Asymmetric Roles of Information, Institutionalization and Diffusion	*Bongani Ngwenya*	413
National Electronic Government Strategies in Austria	*Birgit Oberer and Alptekin Erkollar*	422
Smoke and Mirrors: Can a Useful Approximation of the Cigarette tax gap be Determined?	*Clare Omelia*	432
Adopting Web 2.0 in Building Participatory eGovernment: A Perception Contour From Inside the Government	*Ching-Heng Pan and Lichun Chian*	443
Combating Identity Fraud in the Public Domain: Information Strategies for Healthcare and Criminal Justice	*Marijn Plomp and Jan Grijpink*	451
Approaching eGovernment as a Strategic Driver for Improving the Ethical Model: An Empirical Analysis From Business Economics	*Massimo Pollifroni*	459
Public Procurement and Internet-purchasing: the Defence Sector Evidence	*Nataša Pomazalová and Zbyšek Korecki*	469
Evaluating the Development of eGovernment Systems: The Case of Polish Local Government Websites	*Leszek Porębski*	475
Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach	*Oscar Rebollo, Daniel Mellado, Luis Enrique Sánchez and Eduardo Fernández-Medina*	482
Web 2.0 on the Mexican State Sites: An Overview	*Rodrigo Sandoval Almazán, Gabriela Díaz Murillo, Ramón Gil-Garcia, Luis Luna-Reyes and Dolores Luna-Reyes*	491
eGovernment in Serbia: Prospects and Challenges	*Laslo Šereš and Ivana Horvat*	502
An Organizational Framework for Managing eGovernment Systems in Developing Countries: The Case of Kurdistan Region of Iraq	*Shareef Shareef, Elias Pimenidis, Hamid Jahankhani and J. Arreymbi*	513
Outsourcing of IT Projects in the Public Sector – Sustainable Solution or Erosion of the Public Sector?	*Dalibor Stanimirovic and Mirko Vintar*	522
Closing the Digital Divide gap in European Union: A Unique Solution for Different Tiers?	*Virgil Stoica and Andrei Ilas*	531
Towards Estimating Users' Strength of Opinion in Forum Texts about Governmental Decisions	*George Stylios, Christos KatsisVasiliki Simaki, Sofia Stamou and Dimitris Christodoulakis*	547
An Efficient, Effective eGovernment Enterprise Resource Planning Model	*John Douglas Thomson*	553
Citizen-Government Interaction in Russia: eGovernment as Tradition Bearer	*Anna Trakhtenberg*	564
eGovernment Openness Index	*Nataša Veljković, Sanja Bogdanović-Dinić and Leonid Stoimenov*	571

Paper Title	*Author(s)*	Page No.
Exploring Facilitators and Challenges Facing ICT4D in Tanzania	*Jim Yonazi*	578
PHD		**589**
Maturity Models Transition from eGovernment Interoperability to T-Government: Restyling Dynamic Public Services Through Integrated Transformation of Service Delivery	*Mohamed Mohyi Eddine El Aichi and Mohamed Dafir Ech-Cherif El Kettani*	591
Quality of Services and Citizen Profiling in eGovernment	*Guillaume Gronier, Sandrine Reiter and Mélanie Becker*	603
A Quest for an Applicable Model of Growth for Directgov	*Panos Hahamis*	612
Non Academics Papers		**621**
Providing Public Services Through Digital Postal Networks: A Position Paper	*Liam Church and Maria Moloney*	623
An Evaluation of Expression of Doubt in the context of Self-Assessment: Section 955(4) Taxes Consolidation Act 1997	*Anne Corbett and Francis Rossney*	630
Moving Fast Forward to National Data Standardization	*Asanee Kawtrakul, Intiraporn Mulasastra, Tawa Khampachua and Somchoke Ruengittinun*	643
Work in Progress		**655**
Bridging the IT/Process Divide in Public Administrations by Simple Semantic Interoperability Artefacts	*Robert Orlowski and Veit Jahns*	657

Preface

These proceedings represent the work of presenters at the 11th European Conference on e-Government (ECEG 2011).

The Conference this year is being hosted by the Faculty of Administration, University of Ljubljana, Ljubljana, Slovenia. The Conference Chair is Professor Maja Klun and the Programme Co-Chairs are Mitja Decman and Tina Jukić, all from the University of Ljubljana.

The opening keynote address is given by Dr. Aleš Dobnikar, E-Government and Administrative Processes Directorate, Ministry of Public Administration, Slovenia.

This Conference brings together practitioners and researchers in the area of e-Government from some 40 different countries. Participants will be able to share their research findings and explore the latest developments and trends in the field which can then be disseminated in the wider community.

With an initial submission of 192 abstracts, after the double blind, peer review process there are 74 papers published in these Conference Proceedings. These papers represent research from countries including Australia, Austria, Belgium, Brazil, Canada, Czech Republic, Eygpt, Estonia, Finland, France, Germany, Greece, India, Ireland, Italy, Jordan, Latvia, Luxembourg, Macao, Malaysia, Mexico, Norway, Poland, Romania, Russia, Saudi Arabia, Serbia, Slovenia, South Africa, Spain, Sweden, Taiwan, Tanzania, Thailand, The Netherlands, Turkey, UK, USA and Zimbabwe. This will ensure a very interesting two days.

I hope that you have an stimulating conference, and enjoy your time in Ljubljana.

Maja Klun, Mitja Decman and Tina Jukić
Co-Programme Chairs
University of Ljubljana
June 2011

Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach

Oscar Rebollo[1], Daniel Mellado[2], Luis Enrique Sánchez[2] and Eduardo Fernández-Medina[2]
[1]Social Security IT Management, Ministry of Labour and Immigration, Madrid, Spain
[2]GSyA Research Group, University of Castilla-La Mancha, Spain
orebollo@gmail.com
damefe@esdebian.org
LuisE.Sanchez@uclm.es
Eduardo.FdezMedina@uclm.es

Abstract: Security awareness has spread inside many organizations leading them to tackle information security not just as a technical matter, but from a corporate point of view. Information Security Governance (ISG) provides enterprises with means of dealing with the security of their information assets in a comprehensive manner, involving every stakeholder through the whole governance and management processes. Boards of Public Entities cannot remain unaware of this development and should make efforts to include ISG in their business processes. Realizing this relevant role, scientific literature contains a variety of proposals which define different frameworks to foster ISG inside any corporation. In order to facilitate the adoption of any of them by the public sector, this paper compiles existing approaches, highlighting the main contributions and characteristics of each one. Senior executives and security managers may need support on their decisions about adopting one of these frameworks, so a comparative analysis is performed. Although some comparative reviews are found in literature, they lack a systematic and repeatable methodology, ignore recently published contributions or focus on specific areas, making results biased and inappropriate for general use in corporations and the public sector. This paper tries to guarantee an objective comparison through a set of comparative criteria that have been defined and applied to every proposal, so that strengths and weaknesses of each one can be pointed out. These criteria have been selected from a deep analysis of existing ISG papers, including both governance and management aspects. As results show, each proposal focuses on different aspects of ISG giving priority to some of the defined criteria, and none of them covers the entire required spectrum. Most of the selected frameworks can be used by any public organization as a starting point towards integrating security into their processes, but this paper helps managers to be aware of their limitations and the gaps which need to be covered in order to achieve a complete integration. Consequently, more investigation is needed to fulfill detected gaps and define an ISG framework that organizations can rely on, and which offers security guarantees of covering every information asset of the company. Public sector´s idiosyncrasy must be taken into account in this development, resulting in a general framework eligible for adoption by both public and private companies.

Keywords: information security governance, security governance, comparative analysis, review, governance framework

1. Introduction

Information Technology (IT) security can no longer be considered as a technical issue that can be assessed through hardware implementations, but it is a process that involves the whole company (Pasquinucci, 2007). It is widely accepted that security needs to reach the governance level so that senior directors understand the risks and the opportunities, and have assurance that these are being properly and continuously managed (Williams, 2001). The motivations to introduce IT in the corporate executive agenda is twofold: many countries have developed legislation to hold responsibilities for security breaches (BSA, 2003, Hardy, 2006), and achieving a higher security degree may become a competitive advantage to the organization (Humphreys, 2008, Johnston and Hale, 2009).

Public entities are also involved with these considerations, as higher IT security usually strengthens the trust relationship between Administrations and their citizens. A recent European Union research shows existing gaps related to security and privacy concerns that need to be fulfilled in the field of electronic governance and policy modelling (Crossroad, 2010).

All these objectives may be achieved through Information Security Governance (ISG) which is an overarching category directly affecting the entire policy management process (Knapp et al., 2009). There is not a unique definition of ISG, but among the most widespread conceptions it is generally accepted that ISG consists of the leadership, organizational structures and processes that safeguard information (ITGI, 2006b). ISG can also be defined more specifically as the process of establishing and maintaining a

framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk (Bowen et al., 2006). Finally, focusing on the stakeholders' roles, ISG consists of the frameworks for decision-making and performance measurement that Board of Directors and Executive Management implement to fulfil their responsibility of providing oversight, as part of their overall responsibility for protecting stakeholder value, for effective implementation of Information Security in their Organization (Rastogi and Solms, 2006).

In order to secure their information assets, companies need to adopt an ISG framework that assures effective implementation and makes process operational (Corporate Governance Task Force, 2004). Although there exist a variety of proposed frameworks, organizations neither know which one to adopt nor which one tailors to their own necessities. To help managers in their decisions, the following three comparative reviews have been found: (Rastogi and Solms, 2006) provide existing guidance on ISG and use four frameworks to propose a new definition of ISG; (Park et al., 2006) develop a literature review to look for ISG definitions and use this research to find which security management approaches cover governance success factors, and to know their limitations; (Mahncke et al., 2009) offer a literature review of approaches to measure ISG, and evaluate their suitability to general medical practice.

Existing literature reviews do not compare the proposals in a systematic comprehensive manner, so an additional effort has been performed, presenting the results in this paper. This analysis will show the most relevant ISG frameworks, their characteristics, and the gaps that need to be filled in by future research. Achieved results may help security professionals identify the proposal that best suits their organizations; and lay the foundations of new researches focused on the thorough development of these frameworks.

The research has lead to a set of criteria that allow performing an objective comparison and the repeatability of the results. These criteria have been selected from existing ISG definitions through the extraction of compulsory and desirable features that every framework should accomplish.

During the process, specific and differentiating characteristics of the public sector are taken into account. While E-government is subject to the same threats as e-business, E-government operates within different constraints(Stibbe, 2005). Government entities exist for the purpose of serving society, while commercial firms exist for the benefit of their shareholders (Conklin and White, 2006); therefore the resulting security implementation must have specific considerations. Public organizations may be bound to security considerations according to applicable legislation, but an ISG framework can complement them or even be a substitute in case of lack of regulation (Ozkan and Karabacak, 2010).

This paper is structured as follows: next section offers a brief description of the nine frameworks that have been studied; section 3 presents the comparative criteria that have been defined and the analysis performed; finally, our conclusions and future work are set out in section 4.

2. Information security governance approaches

A literature review has been carried out in depth to locate existing ISG frameworks. The nine most relevant ones are summarized in this section.

2.1 A practical guide to implement and control Information security governance

In (de Oliveira Alves et al., 2006), authors propose a framework for implementing ISG. It focuses on selecting metrics and indicators to track information security evolution, and also on measuring the maturity level of information security inside the organization.

The approach considers the integration of corporate governance indicators, such as Balance Scorecard, with IT and security governance best practices, such as those included in COBIT and ISO/IEC 17799. The practical guide to implement ISG is composed of five stages, which are divided into activities, detailing the actions to be taken and who is responsible for performing each one.

2.2 Business Software Alliance

The Business Software Alliance (BSA) formed the Information Security Governance Task Force whose goal is to frame a response in terms that organizations can understand and implement. This Task Force

has resumed in two white papers many ideas and concepts contained in other reports, legislation and guidelines.

Firstly, in (BSA, 2003), authors state that there is already a legislative and regulatory regime around IT security and it must be enough so that companies stop treating security as a technology issue and start dealing with it as a corporate governance issue. They recommend adopting best practices and standard procedures such as ISO/IEC 17799 (later included in ISO/IEC 27000 family) and recognize the lack of an ISG framework that organizations can adopt. The Task Force proposes a framework where each management role knows what its functions are, how to accomplish its objectives and how to measure and audit the activities performed.

Secondly, the proposal (Corporate Governance Task Force, 2004) expands the framework formerly introduced detailing the functions and responsibilities of every stakeholder involved in security. To implement this framework, authors propose the IDEAL model which is based on five steps: Initiating, Diagnosing, Establishing, Acting and Learning. Finally, tools are provided for the assessment, verification and compliance of the corresponding implementation.

2.3 Information security policy: An organizational-level process model

The proposal (Knapp et al., 2009) focuses on the policy side of ISG. Following a different approach from other studies, authors' methodology includes data collection from security experts and some interviews and questionnaires with security professionals. The result is an information security policy model based on a set of interrelated processes that can be implemented in a repeatable cycle.

Similar to other governance proposals, the model considers the impact of external and internal influences, as well as the role of corporate governance. Also, there is a great emphasis on training and awareness of developed policies through out the whole cycle.

2.4 Information security governance (Von Solms)

Authors have been researching the field of ISG, and as a result they have published a wide variety of papers and a compendium book.

In (Posthumus and Solms, 2004), authors introduce the reason why information security should be considered as a corporate governance issue. They propose an information security framework clearly distinguishing between the governance and management sides.

The approach (Posthumus and Solms, 2006) gives more detail on ISG and Information Security Management, as a part of corporate governance; and describes the tasks, roles and responsibilities of any key individual in an organization.

As stated in (Solms and Solms, 2006), considering that Corporate Governance can be modelled using the Direct-Control Cycle, the same model is applied to Information Security Governance. Each of the steps of this cycle is analyzed through the three management levels: strategic, tactical and operational.

All these results are compiled in the book (Solms and Solms, 2009), where authors describe ISG as part of Corporate Governance and also sharing some aspects of IT Governance. The Direct-Control Cycle anticipated in the previous paper is applied to a group of dimensions of information security and is combined with COBIT and ISO/IEC 27000 as best practices. Also, a methodology of 14 steps is developed to establish an ISG environment.

2.5 ISACA

The Information Systems Audit and Control Association (ISACA) has proposed (ISACA, 2009), where they define a generic model to tackle Information Security within a corporation. The model is based on systems theory and, therefore, consists of processes with inputs and outputs viewed holistically as a complete function unit.

The model has the structure of a tetrahedron with four elements situated in its vertexes and six dynamic interconnections between them that link the elements together. The four elements are:

- Organization Design and Strategy

- People
- Process
- Technology

The six dynamic interconnections are:

- Governing
- Culture
- Enabling and support
- Emergence
- Human factors
- Architecture

2.6 ISO/IEC standards

The International Organization for Standardization (ISO) has a wide portfolio of standards. Among these, the ISO/IEC 27000 family is dedicated to Information Security Management Systems, which can be used by organizations to develop and implement a framework for managing the security of their information assets and prepare for an independent assessment applied to the protection of their information. These standards provide guidelines to protect information assets through defining, achieving, maintaining, and improving information security; what is achieved implementing suitable controls and treating unacceptable information security risks.

Although at first instance, it may seem that this publication only deals with management issues, there are some proposals to integrate them with information security governance. The paper (Solms, 2005) recognizes the broader scope of COBIT, as it covers the whole field of IT Governance, but states that COBIT focuses on what to do but without giving details on how to do it. Here is where the ISO/IEC 27000 family has a chance, as it focuses on Information Security and gives more detail on how to do things. Both frameworks complement each other as shown in (ITGI, 2006a). Standard ISO/IEC 27014, currently under development, pretends to be a proposal on an ISG framework. Its scope includes defining ISG clarifying its relationship with corporate and IT governance; and developing a framework establishing its objectives, principles, and processes. The ISO/IEC 38500 family (ISO/IEC, 2008), which is related to Corporate Governance of information technology, can also be taken into consideration when dealing with ISG. The governance framework proposed in this standard, can be exported to information security implementations.

2.7 ITGI

The IT Governance Institute (ITGI), established in 1998 by the ISACA to focus on original research on IT governance and related topics, has developed COBIT (ITGI, 2007), which is a framework for IT Governance. COBIT 4.1 introduces a set of 34 processes grouped into four domains; detailing the control objectives, metrics, maturity models and other management guidelines for each of these processes. Although COBIT is mainly focused on IT Governance, four of its processes are more related to ISG, namely:

- PO6—Communicate management aims and directions
- PO9—Assess and manage IT risks
- DS4—Ensure continuous service
- DS5—Ensure systems security

Surrounding COBIT, there are a group of products which complement it beyond the main framework (i.e. implementation guide, assurance guide, value of IT investments, etc). The most relevant ones in relation to ISG are the following guides:

- In (ITGI, 2006b) ITGI describes what ISG is and why it is important; details what the Board of Directors and Senior Executives should do, how it can be implemented and what, as consequence, can be achieved.
- The proposal (ITGI, 2008b) is based on the foundations presented in the previous one. It provides more detail on the definition of Information Security Objectives, and the strategies and action plans

that can be used to reach them. Furthermore, critical success factors and metrics are introduced to monitor and measure Information Security, showing that this guide is directed to a lower management level than the aforementioned one.

2.8 NIST

The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, has published many guidelines related to Information Security. The guide (Bowen et al., 2006) has its second chapter dedicated to ISG.

According to this book, there are five components of ISG:

- Strategic Planning
- Organizational Structure
- Roles and Responsibilities
- Enterprise Architecture
- Policies and Guidance

All of these components of governance must be linked to the current implementation of security through on-going monitoring. In order to achieve this result, a description of activities and supporting processes to perform this monitoring is offered. In another NIST publication, (Bowen et al., 2007), the focus points towards developing an Information Security Program, so the key activities of this task are detailed. Among these activities, ISG is highlighted. Also, applicable laws and regulations to security programmes, from the U.S. point of view, are resumed.

2.9 Software engineering institute

The Software Engineering Institute, from the Carnegie Mellon University, has published the guide (Allen and Westby, 2007), as part of the Computer Emergency Response Team (CERT) programme. This guide defines governance for enterprise security and what the characteristics of effective ISG are so that readers can distinguish between effective and ineffective security governance. To succeed on ISG, the guide proposes the definition of an Enterprise Security Program within the corporation. This programme involves personnel at all levels throughout the organization, so different roles are identified pinpointing their functions and responsibilities. Each role has associated a set of activities with their correspondent outputs and supporting documents, which are described in a sequential way.

3. Comparative analysis

This section contains a comparative analysis of the most relevant approaches to Information Security Governance described previously. There is not any standardized framework to compare this kind of proposals so a set of criteria from different research fields will be utilized. These criteria have been selected taking into account the wide variety of existing literature definitions related to ISG. Most of these definitions place this subject as closely linked with IT Governance, Corporate Governance and Information Security, among other areas. Considering these three points of view, a comprehensive group of criteria has been defined, which covers both governance and management aspects.

Selected criteria facilitate performing an objective analysis of the nine identified frameworks. With the proposed comparison topics, the whole spectrum of desirable characteristics related to ISG that can be found in literature is taken into account. To achieve unbiased results, some of the criteria are subdivided into different sub-criteria as a second aggregation level, so that each proposal may be easily classified. Furthermore, besides these three comparison groups, which are shared by every organization, public sector distinct characteristics have been considered. This constitutes a fourth criterion, which reflects the fact that governance processes have their own peculiarities within institutional units. Therefore, the comparative analysis will be based on the criteria detailed in the following subsections.

3.1 IT governance criteria

The literature review shows that there are many definitions of IT Governance. Papers such as (Webb et al., 2006) and (Dahlberg and Kivijärvi, 2006) analyze more than a dozen definitions and highlight five elements, which provide the foundations of IT Governance. These elements are:

- Strategic Alignment: information security must be aligned with business strategy towards the goals of the organization.
- Delivery of business value through IT: optimization of security investments delivering the promised benefits.
- Performance Management: monitoring security strategies to ensure reaching the organization´s goals in time.
- Risk Management: security risk awareness, identifying threats, vulnerabilities and impacts to control and reduce risks over the whole enterprise.
- Control and Accountability: every person in the organization needs to be involved in the security controls and has to know the responsibilities he owns inside the defined framework.

3.2 Corporate governance criteria

As a part of Corporate Governance, the following domains taken from (Simonsson and Johnson, 2006) will be considered:

- Goals: strategy decisions, development of information security policies and guidelines, and controls to monitor whether the goals are achieved.
- Processes: implementation and management of information security processes, with their related activities and procedures.
- People: structure within the organization; defining roles and responsibilities of the different stakeholders.
- Technology: link between Information Security Governance and the physical IT assets that the organization manages (inside and outside).

3.3 Security criteria

Information Security Governance is obviously related to the Information Security field, so a set of security criteria have been selected:

- Standards integration: some proposals refer to controls and best practices included in security standards (i.e. ISO/IEC 27000).
- Information Security Management: policies and procedures defined on the governance side can be linked to the management and operative side of information security.
- Tools and techniques: usually frameworks utilize tools to facilitate their implementation, such as metrics to measure the degree of compliance or maturity models to enable benchmarking between organizations.
- Practical implementation guidelines: theoretical approaches may be distinguished from practical ones; the latter involve detailing implementation activities, including case studies and even practical examples.

3.4 Public sector suitability

Although every identified ISG framework may be adapted to a public organization, some of them include differentiating characteristics that make them more suitable for the public sector. These particularities range from the compliance with specific laws, policies and regulations to requirements originated from multiple governing bodies; going through funding limitations in budgets and investments. Public institutions need to consider security beyond technical aspects in four domains: social, political, cultural and legal (Wimmer and Bredow, 2002). This fourth criterion evaluates these domains so that it may help boards in their decisions, avoiding unnecessary efforts in tailoring an ISG framework to a public entity.

3.5 Analysis results

The former defined criteria have been applied to the nine frameworks presented in section 2. The results are summarized in Table 1, which has been elaborated assigning three levels of conformance (high, medium and low) to each of the criteria.

Table 1: Comparison of ISG frameworks

Criteria / ISG Frameworks	A practical guide to implement and control Information Security Governance	Business Software Alliance	Information security policy: An organizational-level process model	Information Security Governance (Von Solms)	ISACA	ISO Standards	IT Governance Institute	NIST	Software Engineering Institute
IT Governance									
Strategic Alignment	medium	medium	high	medium	high	medium	high	high	high
Delivery of business value through IT	medium	low	low	low	medium	low	high	low	medium
Performance Management	low	medium	medium	medium	medium	high	high	medium	low
Risk Management	high	high	high	high	low	high	high	high	high
Control and Accountability	medium	low	medium	high	low	medium	high	low	high
Corporate Governance									
Goals	medium	medium	high	medium	high	medium	high	high	high
Processes	high	high	high	high	high	high	high	high	high
People	high	high	low	high	high	medium	medium	high	medium
Technology	high	low	medium	medium	high	medium	low	low	medium
Security									
Standards integration	high	medium	low	high	low	high	low	high	medium
Information Security Management	medium	low	medium	high	low	high	medium	medium	medium
Tools and techniques	high	high	medium	low	low	high	medium	low	low
Practical implementation guidelines	medium	high	low	medium	medium	high	low	medium	medium
Public Sector Suitability	low	medium	low	low	low	low	low	high	low

Table results can be analyzed from two different perspectives. On the one hand, horizontally, some of the proposed criteria are more widespread over the ISG frameworks than others. Among the governance criteria, nearly all of the proposals deal with strategic alignment, risk management, goals and processes; however, delivery of business value through IT is only deeply developed by the IT Governance Institute on the Val IT Framework (ITGI, 2008a), and technology relations with physical IT implemented assets are seldom considered. Generally speaking, security criteria seem to be less relevant than the previous ones, as authors tend to offer high level solutions, distant from implementation details.

On the other hand, vertically, three of the frameworks seem to be more aligned with the groups of criteria and could be considered as reference starting points. Namely: IT Governance Institute focuses on IT Governance, ISACA is mainly related to Corporate Governance, and ISO Standards deal principally with Security criteria. The rest of the approaches are situated in intermediate positions, leveraging the importance each one gives to every comparative aspect.

With respect to public sector suitability, most of the frameworks do not detail the specific implications of implementing ISG into a public entity. The guidelines proposed by the NIST are the main exceptions which take into account these considerations, but they are much localized as a consequence of having their foundations based on US regulations and laws. Therefore, additional efforts are needed when adapting this framework to other country´s organizations. Also, some guidance is included in BSA´s proposal, which offers some key notes when adopting information security by educational and non-profit institutions.

Public organizations are usually bound to a specific regulatory framework which results in different governance processes. This is the consequence of the application of the corresponding legislation which emanates from various level authorities (national, regional, etc). In most cases, the selected ISG proposal needs to be localized to the regulations where the organization resides.

4. Conclusions and future work

The security of any organization´s assets must involve every stakeholder from senior executives to operational personnel. Information Security Governance helps to carry out this task providing a framework which can be adopted by enterprises. The board of governance of any company that relies on this methodology should be confident about compliance with a wide set of security measures and even regulation requirements; furthermore, information security becomes a process inside the organization covering all of the information assets and provides alignment with business strategy.

The nine most relevant ISG frameworks existing in the literature have been reviewed in this paper, performing a comparative analysis between them using a comprehensive set of conformance criteria. The performed review has shown that none of the approaches, not even the most recent ones, fulfil every necessity field that organizations need to tackle. Although these proposals include desirable features, their main lacks have been highlighted.

Special attention has been paid to public sector suitability, but most ISG proposals are more focused on private corporations than public organizations. This issue may be considered by the directors of any public institution when adopting one of these methodologies.

Additional research work is needed to develop a general ISG framework which fills the detected gaps. Either taking any of the approaches included in the comparative study as a starting point, or building it from scratch, it is imperative that such a task is undertaken. Future work will follow this line, complementing existing proposals to reduce their weaknesses as well as to achieve a comprehensive framework that can be systematically extended to any organization.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557), financed by the Centre for Industrial Technological Development (CDTI), ORIGIN (IDI-2010043(1-5)) financed by the CDTI and the FEDER, BUSINESS (PET2008-0136) awarded by the Spanish Ministry for Science and Technology and SEGMENT (HITO-09-138) and SISTEMAS (PII2I09-0150-3135) financed by the Council of Education and Science of the Castilla-La Mancha Regional Government.

References

Allen, J. H. & Westby, J. R. (2007) *Governing for Enterprise Security Implementation Guide*, Software Engineering Institute - CERT.

Bowen, P., Chew, E. & Hash, J. (2007) *Information Security Guide For Government Executives*, National Institute of Standards and Technology.

Bowen, P., Hash, J. & Wilson, M. (2006) Information Security Governance. *Information Security Handbook: A Guide for Managers.* National Institute of Standards and Technology.

BSA (2003) *Information Security Governance: Toward a Framework for Action*.

Conklin, A. & White, G. B. (2006) e-Government and Cyber Security: The Role of Cyber Security Exercises. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*.

Corporate Governance Task Force, T. (2004) *Information Security Governance: A Call to Action*.

Crossroad (2010) Updated Gap Analysis Report. *A Participative Roadmap for ICT Research in Electronic Governance and Policy Modelling*.

Dahlberg, T. & Kivijärvi, H. (2006) An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. *Proceedings of the 39th Hawaii International Conference on System Sciences*.

de Oliveira Alves, G. A., Rust da Costa Carmo, L. F. & Ribeiro Dutra de Almeida, A. C. (2006) Enterprise Security Governance: A practical guide to implement and control Information Security Governance. *Business-driven IT Management*.

Hardy, G. (2006) Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report,* 11**,** 55-61.

Humphreys, E. (2008) Information security management standards: Compliance, governance and risk management. *Information Security Technical Report,* 13.

ISACA (2009) *An Introduction to the Business Model for Information Security*.

ISO/IEC (2008) ISO/IEC 38500:2008 Corporate governance of information technology.

ITGI (2006a) *COBIT Mapping to ISO/IEC 17799:2000 With COBIT*.

ITGI (2006b) *Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd Edition)*.

ITGI (2007) *Control Objectives for Information and related Technology (COBIT 4.1)*.

ITGI (2008a) *Governance of Investments, The Val IT Framework 2.0*.

ITGI (2008b) *Information Security Governance: Guidance for Information Security Managers*.

Johnston, A. C. & Hale, R. (2009) Improved Security through Information Security Governance. *Communications of the ACM,* 52**,** 126-129.

Knapp, K. J., R. Franklin Morris, Thomas E. Marshall & Byrd, T. A. (2009) Information security policy: An organizational-level process model. *Computers & Security,* 28**,** 493-508.

Mahncke, R. J., McDermid, D. C. & Williams, P. A. H. (2009) Measuring Information Security Governance Within General Medical Practice. *Proceedings of the 7th Australian Information Security Management Conference.*

Ozkan, S. & Karabacak, B. (2010) Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management,* 30**,** 567-572.

Park, H., Kim, S. & Lee, H. J. (2006) General Drawing of the Integrated Framework for Security Governance. *Lecture Notes in Computer Science,* 4251**,** 1234-1241.

Pasquinucci, A. (2007) Security, risk analysis and governance: a practical approach. *Computer Fraud & Security***,** 12-14.

Posthumus, S. & Solms, R. v. (2004) A framework for the governance of information security. *Computers & Security,* 23**,** 638-646.

Posthumus, S. & Solms, R. v. (2006) A Responsibility Framework for Information Security. *International Federation for Information Processing.*

Rastogi, R. & Solms, R. v. (2006) Information Security Governance - A Re-Definition *IFIP International Federation for Information Processing,* 193**,** 223-236.

Simonsson, M. & Johnson, P. (2006) Assessment of IT Governance - A Prioritization of Cobit. *Proceedings of the Conference on Systems Engineering Research*.

Solms, B. v. (2005) Information Security governance: COBIT or ISO 17799 or both? *Computers & Security,* 24**,** 99-104.

Solms, R. v. & Solms, S. H. B. v. (2006) Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security,* 25**,** 408-412.

Solms, S. H. v. & Solms, R. v. (2009) *Information Security Governance*, Springer.

Stibbe, M. (2005) E-government security. *Infosecurity Today,* 2**,** 8-10.

Webb, P., Pollard, C. & Ridley, G. (2006) Attempting to Define IT Governance: Wisdom or Folly? *Proceedings of the 39th Hawaii International Conference on System Sciences*.

Williams, P. (2001) Information Security Governance. *Information Security Technical Report,* Vol 6, No. 3**,** 60-70.

Wimmer, M. & Bredow, B. v. (2002) A Holistic Approach for Providing Security Solutions in e-Government. *Proceedings of the 35th Hawaii International Conference on System Sciences*.