Preface

IT security can no longer be considered as a technical issue, but it is a process that involves the whole company. 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.

This relevant role assumption has caused the development of a lot of initiatives (frameworks, standards, etc.) in the last few years to foster IT Governance inside any corporation, such as CobiT or ISO/IEC standards (ISO/IEC 27000, ISO/IEC 38500…). From a global perspective, this diversity, also found in the context of security technical issues, has made us consider its application as a very complex and hard process to understand with a very difficult implantation curve.

In order to facilitate the adoption of IT Security Governance by the different types of organizations, the objective of this book is to compile existing approaches, standards, best practices, and new trends in IT Security Governance. The book will highlight the main contributions and characteristics of each one. From the theoretical and practical perspectives, this book is intended to address security during the whole IT Security Governance implantation lifecycle. From IT risk-based security goals and policies up to IT security governance tools and metrics implemented by most sound IT security standards or guidelines for each specific scenario. This book can also help managers to be aware of limitations of current approaches and the gaps which need to be covered in order to achieve a complete integration of the security governance within the global governance.

This book aims to provide a theoretical and academic description of IT security governance issues, and practical and innovative guidelines, standards, models, and frameworks for implementing IT security governance in organizations.

The proposed book could serve as a reference for CEOs and CIOs, security managers, systems specialists, systems architects, security developers, information security professionals, software engineers, project managers, and computer science students.

Finally, this book will allow the knowledge and experience of renowned ICT Governance professionals to be shared, and thus supposes an important reference with which to assist companies to obtain their strategic goals.

GENERAL PICTURE OF INFORMATION TECHNOLOGY GOVERNANCE

Information Technology (IT) Governance is the component of Corporate Governance focused on the management of new technologies inside any organization. As any governance area, it does not only include the lower levels operational aspects, but also the higher tactical and strategical ones, guaranteeing

an alignment of the company's utilization of technologies and IT investment with the global objectives. Its origin arises with the necessity to apply to the company's IT the same procedures that have been developed over other governance areas to foster its competitive advantage, making it essential in today's economy that the board of directors of any organization are responsible of its IT usage. In this book's way to define ISG, it is also important to understand previously IT Governance because, under some perspectives, ISG can be considered a sub-component of IT Governance. As a result, ISG inherits its core characteristics from both Corporate Governance and IT Governance.

What is IT Governance?

A first general approach to IT Governance may be to state that it is the decision rights and accountability framework for encouraging desirable behaviors in the use of IT (Weill and Ross 2004). It is important to highlight from this definition that the responsibility of IT Governance, as any other governance subject, belongs to the board of directors and high executives. Usually this responsibility is delegated on the IT department, but the accountability of the use of IT remains still in the board.

Offering more detail, the ITGI defines IT Governance as *the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives* (ITGI 2003). The responsibility of the board is again mentioned, and positions IT governance as part of the Corporate Governance. As a result, it cannot be considered as an isolated discipline, but in coordination with other governance structures. IT is linked to other organizational key assets (like financial, human, or physical) so it must be included in the same decision making processes.

Other definitions can be found on literature, but most of them focus on the same highlighted aspects. Summarizing, in (Webb, Pollard, et al., 2006) twelve other definitions are analyzed to suggest the following one that unifies the main concepts: *IT Governance is the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management*. In developing this definition, authors realize that IT Governance shares many similarities with Corporate Governance and with Strategic Information Systems Planning. This analysis shows that IT Governance is built upon five elements, which are:

- Strategic Alignment.
- Delivery of business value through IT.
- Performance Management.
- Risk Management.
- Control and Accountability.

These five elements are aligned with the ITGI statement which indicates that IT Governance's purpose is to direct IT endeavours, to ensure that IT's performance meets the following objectives:

- Alignment of IT with the enterprise and realisation of the promised benefits.
- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits.
- Responsible use of IT resources.
- Appropriate management of IT-related risks.

The same as Corporate Governance is conformed by multiple sub-governance areas, one of which is IT Governance; IT Governance itself can be subdivided in multiple governance components. Some examples of these areas are: Performance and Capacity Governance, IT Services Governance, IT Resources Governance, and Information Security Governance (ISG).

Why is IT Governance Important?

Information Technologies have become an essential element of every business, showing the potential of offering new opportunities to obtain competitive advantages and increase productivity. These new technologies have burst into traditional procedures transforming them so that more efficient results are obtained and more value is created with the same resources. Even more, the widespread use of IT has allowed the creation and delivering of new market services based fundamentally on intangible assets such as information, knowledge trust or reputation. Therefore, it is of paramount importance an effective governance of IT to achieve enterprise goals.

Although these new technologies are fundamental to sustain many business operations, they also generate new risks. A sight on how strongly enterprises rely on IT is enough to understand the dependence generated by most companies on the new networked economy. With IT so intrinsically imbricate within enterprises, boards of directors need to analyze it specifically to determine how it can contribute to the execution of the business strategy. Therefore, IT reaches the strategic decision level because of its contribution to the company's growth and innovation, and its support to the organization's objectives.

Despite the importance of the IT risks generated and the high volume of investments associated with IT, traditionally it has not been an issue tackled by the board of directors. In doing so, the governance body cannot expect to deliver quality IT solutions on time and budget, and business losses may appear in the form of higher costs, damaged reputations, or less efficient core processes. IT has been usually derived to technical departments and treated separately of the business as an independent area, which has proven a poor governance strategy.

Best Practices on IT Governance

To finish the discussion on IT Governance, the authors introduce existing proposals of best practices on this subject. Although several guidelines and recommendations exist in literature over IT Governance, the most widespread one is Control Objectives for Information and related Technology (CobiT), developed by the ITGI (ITGI 2007). CobiT introduces a framework for IT Governance which is built upon a set of 34 high level processes grouped into four domains; detailing the control objectives, metrics, maturity models, and other management guidelines for each of these processes.

The 34 high level processes are grouped into the following domains:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

These domains can be followed in an iterative cycle through which the defined processes are successively executed to achieve adequate governance.

CobiT has become a “de facto” standard for IT auditing, offering a structured guideline of relevant processes and control objectives that need to be analyzed within the IT auditory. But going a step further from an auditing tool to an IT Governance tool, CobiT can be used by any company to achieve a higher degree of IT Governance. An organization may choose which of the 34 processes decides to implement and follow its control objectives to guarantee its success. Also, once the processes are deployed, CobiT’s maturity models offer a benchmarking of the fulfilment degree of each matter inside the enterprise, which can result in a performance indicator of IT Governance.

CobiT framework identifies five focus areas on IT Governance:

- Strategic alignment
- Value delivery
- Resource management
- Risk management
- Performance measurement

These five areas are clearly aligned with the five elements of IT Governance highlighted when the definition was presented.

OVERVIEW OF INFORMATION security GOVERNANCE

Information Security Governance (ISG) is focused in the appropriate governance and management of any company’s information assets. As indicated in the previous section, ISG is broadly considered a component of IT Governance because many Information Security aspects are related with IT (electronic data bases, information systems, etc.). But ISG is also considered a direct component of Corporate Governance, when dealing with aspects not related with IT; for example with legal issues, human resources or physical security. This double dependence appears because of the multidimensional nature of Information Security, which in many ways relies on IT procedures, but also includes some separate aspects.

Introduction to Information Security

Information has become a critical asset of any organization. The fast adoption of IT by all the business activities of every enterprise has arisen the necessity to manage carefully the company’s information. Nowadays, information is an asset as important as capital or work. This reality is even more pressing on new generation companies in which information is part of their core business.

Enterprise security is a classical term that reflects the efforts performed to avoid business risks, letting the company to surpass any threat that may jeopardize its survival. The traditional security concept needs to be expanded in order to include the mentioned information assets, whose combination is known as Information Security.

Security and information are therefore two closely linked terms, which is shown in the fact that any company’s information is as good as the security mechanisms it has implemented over it. Unreliable information due to wrong security policies generates uncertainty and mistrust, impacting negatively on every business area. Otherwise, secure information is a sign of certainty which contributes to generate value inside and outside the company.

Information Security is a business function whose mission is to establish security policies and their associated procedures and control elements over their information assets, with the goal of guaranteeing their authenticity, confidentiality, availability and integrity. Ensuring these four characteristics is the core function of Information Security:

- Authenticity allows trustful operations by guaranteeing that the handler of information is whoever it claims to be
- Confidentiality is understood in the sense that only authorized users access the information, avoiding its spreading among users without the proper rights
- Availability refers to being able of accessing information whenever is necessary, guaranteeing that offered services can be used when needed
- Integrity is the quality which shows that the information has not been modified by third parties, and assures its correctness and completeness

As stated previously, Information Security has a multidimensional nature because it involves many different subjects that must be implemented coordinately in order to secure the information assets. In (Solms and Solms 2009) authors identify a list of dimensions, some of which are:

- Governance Dimension
- Management Dimension
- Ethical Dimension
- Legal Dimension
- Insurance Dimension
- Personnel/Human Dimension
- Technical Dimension
- Audit Dimension
- IT Forensics Dimension

The elements of this list may be clearly differentiated between those related with IT and those more connected to other enterprise areas. This is the reason why Information Security, although very linked with IT, goes beyond its boundaries into other crucial aspects. This point of view of Information Security is developed in the following section to introduce a definition of ISG.

What is Information Security Governance?

After introducing Corporate Governance and IT Governance we are now in conditions of understanding Information Security Governance (ISG) as part of the governance activities that every enterprise should develop. Through the previous steps of this introduction, we have positioned ISG under the concepts of both Corporate Governance and IT Governance. So having set the scope of ISG, it is time to continue with its definition.

A first approach to ISG is given by the ITGI: *Information security governance consists of the leadership, organisational structures and processes that safeguard information. Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manage risks appropriately, uses organisational resources responsibly, and monitors*

the success or failure of the enterprise security programme (ITGI 2006). This definition stresses the dependency of ISG with respect to Corporate Governance, and includes the global objectives proposed in IT Governance, which are inherited (strategic alignment, risk management, resource management, performance measurement, and value delivery).

Following the governance argumentation, ISG can be defined as *an overarching category directly affecting the entire policy management process; doing so also stresses that governance is not merely an internal organizational process but can consist of external attributes such as the involvement of a board of directors* (Knapp, Morris et al. 2009). In this case, authors highlight that the governance aspect is not just some internal matter of the company, but it must be projected to its exterior.

A clear introduction of the stakeholders' roles can be found in (Rastogi and Solms 2006): *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*. Therefore, the responsibility of the board of directors and high executives within ISG is unquestionable, as with other governance areas.

The National Institute of Standards and Technology (NIST) proposes: *ISG can be defined 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, Hash, et al., 2006). This approach focuses on the compliance on current legislation, due to the public nature of the NIST, and also introduces the concept of risk management specifically applied to Information Security.

Finally, deepening in its relationship with Information Security, ISG is defined as *the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems* (Moulton and Coles 2003), where the main objectives of Information Security are recalled (confidentiality, integrity, and availability).

Why is Information Security Governance Important?

A direct consequence of the multidimensional nature of Information Security, it can no longer be considered just as a technical issue that can be assessed through hardware implementations, but as a process that involves the whole company (Pasquinucci 2007). Responsibility for security management has traditionally been limited to operational and technical managers, but it is essential to extend it to the governance levels. A greater involvement of boards of directors, executive management and business process owners is required, so that senior directors understand the risks and opportunities, and assure that these are being properly and continuously managed (Williams 2001).

A first motivation to introduce Information Security into the governance level is explained by the legal responsibility for security breaches. Both companies and individuals are everyday more aware of the necessity of increasing security in everyday activities. This increasing concern has not only forced companies to tackle this security issues, but has also reached legislators to take action. Actually, governments have already established a significant legislative and regulatory regime around Information Security (BSA 2003), most of which focus the security responsibilities around the governance bodies. The main drawback, especially for non-local organizations, is that no uniform regulatory framework exists in every country, so that the ISG area must consider specific implications of each applicable region.

Besides legal constrictions, information assets are too valuable for any enterprise to allow unnecessary risks that can threaten its own survival. On the one hand, security breaches can damage seriously the image of the firm, which is not easily recovered, or can result in substantial penalties. On the other hand, an adequate management of Information Security and its related assets may be perceived positively by clients and result in a competitive advantage to the organization.

When Information Security is addressed at the corporate level as part of the enterprise planning process, it is afforded greater ownership by employees of the firm. Greater ownership means that employees are more responsible and accountable for the security of their assets, and view security not as a barrier to success, but as an enabler. Improved ownership also contributes to an organizational culture of secure computing (Johnston and Hale 2009).

Therefore, developing an ISG programme is not just a matter of legal compliance, but an investment on the company's self-interest. However, when organizations delegate Information Security on lower management and technical levels, they can not expect to receive enough attention in proportion to the magnitude of the handled risks. These intermediate levels usually do not have at their disposal the budgets to tackle these security threats, and lack of the decision level to manage these responsibilities.

Additionally, to help organizations in implementing ISG there have been developed numerous guidelines. Each approach focuses on different specific aspects of ISG, but it does not exist a recognized standard that may aid companies defining what activities should be accomplished and how to perform them.

AIMS OF THIS BOOK

This book aims to provide a theoretical and academic description of IT Security Governance issues, and practical and innovative guidelines, models and techniques for implementing IT security governance practices in organizations.

The book covers the following topics:

- An in-depth review of the major IT security governance frameworks, IT security governance legal issues, and IT security governance overview in e-banking.
- Approaches based on main IT security governance standards, guidelines, and models, both theoretical and practical perspectives, will be presented.
- Practical and innovative guidelines, models, and techniques for implementing IT security governance practices in organizations will be described.

ORGANIZATION OF THIS BOOK

This book is divided into three sections and eleven chapters, each section addressing a state-of-the-art topic in IT Security Governance. They are as follows: IT Security Governance Landscape, Security Standards and Guidelines in the IT Security Governance, and IT Security Governance Innovations.

Section 1: IT Security Governance Landscape

1. Overview of Key Information Security Governance Frameworks

This chapter tries to provide an overview of state of the art of the most current relevant security governance frameworks by means of a 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. Most of the selected frameworks can be used as a starting point towards integrating security inside their processes, but this paper helps managers to be aware of its limitations and the gaps which need to be covered in order to achieve a complete integration.

2. IT Security Governance in E-Banking

In this chapter the authors are focused on an analysis of reputed best standards, guidelines on governance, Risk Management methods, and internal controls currently used for e-banking (one of the most important sectors in IT security governance) as means to research which satisfies best Information Security Governance (ISG) objectives. They propose an ITSG framework for e-banking as a continuous process for assuring ISG objectives. They also highlight the importance of consistent measurement of metrics of ITSG performance with the aid of Security Content Automation Protocol.

3. IT Security Governance Legal Issues

IT must fulfill the privacy protection regulations currently in force and the companies using it must carry out the international auditing standards. But intellectual property rights cannot protect simple data and information, apart from the substantial investment made in either obtaining, verification or presentation of data, by sui generis right over databases (or database right). This chapter examines and compares the current legislations of developed countries in order to find the characteristics -and the criticism- in common.

Section 2: Security Standards and Guidelines in the IT Security Governance

4. Information Technology Service Management

ITIL® (Information Technology Infrastructure Library) is the most used and extended model related to IT service management. The purpose of this chapter is to describe briefly the main phases and processes related to the ITIL® service lifecycle, detailed information related to the information security management process, and the qualifying system for IT Service Management with ITIL®, with regard to IT Security Governance.

5. Assessing the Maturity of Control Objectives for Information and Related Technology (COBIT) Framework in the Egyptian Banking Sector

Banking sector is one of the most important sectors in IT security governance and in Egypt is one of the largest business sectors in terms of contributing to country economic growth and in terms

of investing in IT. Thus, implementing a good IT security governance framework inside Egyptian banks is a rather critical issue. The purpose of this chapter is to assess the importance and the implementation of Control Objectives for Information and Related Technology (COBIT) high level processes in the Egyptian banking sector under a practical perspective.

6. Adoption of ISO 27001 in Cyprus Enterprises: Current State and Challenges

This chapter presents the findings of an investigation on current IT security governance practices in Cypriot organizations, including enterprises and public sector divisions. In order to gain knowledge on the deployed security technologies by organizations, a survey was conducted and concluded in late 2010. The survey primarily examined compliance of enterprise current security policies and procedures with ISO/IEC 27001 security guidelines. A research analysis has been performed, which identified that security mechanisms and the management of IT resources may be improved on a number of aspects. Based on the research findings, an assessment of the viability of ISO/IEC 27001 in Cyprus is given as well as recommendations on the further deployment of ISO/IEC 27001.

7. An Information Governance Model for Information Security Management

The purpose of this chapter is to propose an IS security governance model to enhance the security of information systems in an organisation by viewing security from a holistic perspective of encompassing information security, information assurance, audit, governance and compliance. This is achieved through the strategic integration of appropriate frameworks, models, and concepts in information governance, IS service management, and information security. The frameworks identified are Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL), ISO 27002, Risk IT and Payment Card Industry Data Security Standard (PCI DSS).

Section 3: IT Security Governance Innovations

8. Information Security Governance Using Biometrics

To establish the identity of an individual is very critical with the advancement of technology in networked society. Thus there is need for reliable user authentication technique to solve the growing demand for high level of Information Security Governance (ISG) depending on the requirement. Biometrics can be explained as the method to recognize an individual based on physical (face, fingerprint, ear, iris, etc.) or behavioral (voice, signature, gait, etc.) to identify an individual person. Nowadays, biometric systems are being used for different purposes for information security like commercial, defense, government, and forensic applications as a means of establishing identity and to mitigate the risk which is one of the important objectives of Information Security Governance. In this book chapter, an attempt has been made to explain the use and proper selection of biometric trait to help in Information Security Governance.

9. Ontology Based Multi Agent Modelling for Information Security Measurement

In this chapter the authors discuss a framework for building a multi agent information model that captures the notion of compliance semantics and present it using event ontology. The authors also present a methodology for computing the compliance measure of organizational practice with regulatory/standards requirements capturing the relevance of the ontological concepts using fuzzy weights towards estimating the compliance. Without any loss of generality the authors show their technique applied in some particular cases of Information Technology - Security Techniques (AS/NZS ISO/IEC 17799:2006 & CobiT4.1) where the authors present an ontology, construct semantic model, and derive compliance rules from the information security controls. Finally the authors compare the two standards and discuss how the model can be used as a decision support system tool at the hands of auditors in the chosen domain in order to improve the auditory of the security governance of Information Systems.

10. Using Indicators to Monitor Security Risk in Systems of Systems: How to Capture and Measure the Impact of Service Dependencies on the Security of Provided Services

In this chapter, the authors put forward a method for the capture and monitoring of impact of service dependencies on the security of provided services. The method is divided into four main steps focusing on documenting the system of systems and it service dependencies, establishing the impact of service dependencies on risk to security of provided services, identifying measureable indicators for dynamic monitoring, and specifying their design and deployment, respectively. The authors illustrate the method in an example-driven fashion based on a case within power supply.

11. Information Security Governance: The Art of Detecting Hidden Malware.

The goal of this chapter is, firstly to unearth the recent obfuscation strategies employed to hide malware. Secondly, this chapter proposes innovative techniques that are implemented as a fully-automated tool, and experimentally tested to exhaustively detect hidden malware that leverage on system vulnerabilities. Based on these research investigations, the chapter also arrives at an information security governance plan that would aid in addressing the current and future cyber-crime situations.

Daniel Mellado
Rey Juan Carlos University, Spain

Luis Enrique Sánchez
University of Castilla – La Mancha, Spain

Eduardo Fernández-Medina
University of Castilla – La Mancha, Spain

Mario Piattini
University of Castilla – La Mancha, Spain

REFERENCES

Bowen, P., & Hash, J. (2006). Information security governance . In *Information security handbook: A guide for managers* (pp. 2–19). National Institute of Standards and Technology.

BSA. (2003). *Information security governance: Toward a framework for action.*

ITGI. (2003). *Board briefing on IT governance* (2nd ed.).

ITGI. (2006). *Information security governance: Guidance for boards of directors and executive management* (2nd ed.).

ITGI. (2007). *Control objectives for information and related technology* (COBIT 4.1).

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*, 126–129.

Knapp, K. J., & Morris, M. F. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*, 493–508.

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7).

OECD. (2004). *OECD principles of corporate governance*.

Pasquinucci, A. (2007). Security, risk analysis and governance: A practical approach. *Computer Fraud & Security*, *7*, 12–14.

Rastogi, R., & van Solms, R. (2006). Information security governance - A re-definition. *International Federation for Information Processing*, *193*, 223–236.

van Solms, S. H., & van Solms, R. (2009). *Information security governance*. Springer.

Webb, P., Pollard, C., et al. (2006). Attempting to define IT governance: Wisdom or folly? *Proceedings of the 39th Hawaii International Conference on System Sciences*.

Weill, P., & Ross, J. W. (2004). *IT governance on one page*.

Wikipedia. (2011). *Corporate governance*. Retrieved from http://en.wikipedia.org/wiki/Corporate_governance

Williams, P. (2001). Information security governance. *Information Security Technical Report*, *6*(3), 60–70.