

INFORMATION SECURITY GOVERNANCE

By Aljosa PASIC, Pedro SORIA RODRIGUEZ and Javier CALVO TORRES

Atos Research and Innovation, Atos Origin sae, Albarracin 25, 28037 Madrid, Spain

SECURITY AND ORGANIZATIONAL GOVERNANCE

Information Security Governance and its alignment with the overall organizational governance is certainly not a new issue. In [1] a number of issues and best practises have been listed, such as:

- Who Should Be Concerned With Information Security Governance?
- What should be Outcomes?
- How to Find Out How Management Addresses Information Security Issues?
- How to Self-assess Information Security Governance Practices?
- etc

In a survey [2] done by Atos Origin and the National Computing Centre in United Kingdom, the need for integration from fragmented governance which doesn't align security under the influence of CISOs (chief information security officer) has been pinpointed, together with a evidence that organisations are recognising that security and information risk issues merit additional investment. However, same report states that without the will to integrate the way risk is managed across the enterprise much of this additional investment will lack focus and crucially fail to deliver the returns. What we need is an aligned, streamlined and integrated governance model that is, at the same time, resilient to emerging organisational, technological and information security changes.

Organizational changes might often follow regulation and compliance requirements, such as the recent cases of the finance function and Chief Financial Officer Role & responsibility changes. Another Atos Origin report [3], states that the key to implement changes in governance is not just as 'one-off' silo requirements, but in as smart and intelligent way that spans over different governance layers. In order to integrate related governance layers and issues, companies must also move from periodic review to continual and ongoing governance monitoring, including the use of tools for automated compliance checking.

When it comes to technological and security changes and future challenges, we should underline the belief that security must be forethought and "built-in" component, rather than "add-on" component. This belief acknowledges the need for integrating security into the early design and development phases of information systems, which imposes new constraint on alignment and integration of ICT and security Governance levels. Moreover, in the current Information Security Governance models, security requirements are often identified independently for various system components, such as network layer, server storage and computing resources, processing of sensitive data etc without explicitly considering the interdependences between them and the alignment with ICT and organisational (corporate) governance. In addition, security governance often envisages only a single context, which for the future service oriented applications and systems seems inappropriate.

In [4] authors describe eleven “Characteristics of Effective Security Governance”, and they describe that “determining how much security is enough is based upon the risk exposure an organization is willing to tolerate, including compliance and liability risks, operational disruptions, reputational harm, and financial loss.” They also state that one of the best measures that an organization is addressing security as both a governance and management concern is that leaders regularly promulgate a set of beliefs, behaviours, capabilities, and actions that are consistent with security best practices and standards.

From this and other related papers ([5], [6], [7] and [8]) it becomes obvious that some of the essential tasks in governance are related to risk management and compliance, and that here might be an opportunity for software automation: to track projects, gather evidence, store relevant documents, survey risky activity, determine controls effectiveness, and so forth. In matter of fact, there are already many vendors whose solutions target some of these functions of organizational, ICT and Information Security governance. Transparency, one of the governance objectives at all layers, is for example created through feedback from people and processes, and automation tools (also called compliance orchestration tools or controls monitoring products) can actually collect raw data about IT systems or security processes and indicate whether controls have failed. There are also other tools for analysis, tracking key indicators and control objectives, report creation, visualisation etc. However, in order to fulfil our vision of aligned, streamlined and integrated governance, we need all these tools to exchange information more frequently in a roundtrip fashion, we need to “operationalise” compliance rules (i.e. transform them into “executable” security controls), to integrate risk management knowledgebase for all governance levels etc.

ALIGNMENT OF GOVERNANCE LEVELS IN SOA ENVIRONMENT

In the wake of the age of Service Oriented Architectures (SOA), the interplay of the different levels of Governance becomes more relevant for global enterprises. By exploiting an SOA, the IT infrastructure can be structured around loosely coupled and distributed business processes, and thus achieving more efficient implementation of those business processes. Corporate governance and IT governance become more strongly interrelated when utilizing SOAs, and as such, the two governance models need to be aligned for optimum results.

Security requirements and implementation or adaptation of different security mechanisms must also be in line with changes derived from this new environment. The nature of SOA, with highly dynamic and distributed software components, storage and computing resources imposes some important requirements: a typical plan-do-check-act security management cycle must now comply with higher Governance levels and must have much shorter iteration cycle. Security requirements, for example, need to take into account the close relationships and interplay between business and SOA infrastructure levels. Activities that might have been spread across organization, such as the monitoring of security measures and the evaluation of security threats, now have to be encompassed within the global information security governance practice. In addition, as we stated earlier, there is a growing need to align the Corporate, IT and Security governance levels of an organization.

While such alignment is desirable, it is often an underdeveloped goal, as each governance level falls often under the responsibility of different positions within an enterprise, usually with little coordination of the security roles and responsibilities with the other two levels of governance. Take for example, information security risk and its poor alignment with the overall organizational risk objectives. While many global organizations are these days consciously taking more risks, in order to create new opportunities and increase business potential, information security risk managers are often taking opposite direction, considering risk “something to avoid” and focusing their perspective on loss

limitation. As SOA is making their job and decision making even more complex, with infrastructures going open and global, there is an obvious need to balance various points of view from different Governance levels. The other example is related to cost decision making. From the past we know that when the things go bad in an organization, cost centers like IT and security are among the first to experience budget reductions. This results in tighter resources available to effectively operate the IT infrastructure and to manage the security, ultimately affecting organizational response to the new and emerging threats. If something unpredicted happens, e.g. denial of service attack that harms organizational reputation, governance investment decisions act like a boomerang, damaging the main governance target: business value.

SOA environment is indeed helping global organizations to make the best use of their distributed IT resources while achieving maximum flexibility and efficiency; but the alignment of the different governance levels, that used to be a recommendation, now becomes almost an obligatory property of the global enterprise. In addition, SOA is a distributed environment that yields global governance that goes beyond enterprise risk reduction. Whilst spending on security has grown in response to increasing risk, the issues such as identity theft, privacy breach, fraud, etc often global issues/processes that cannot be solved with the traditional focus on technical solutions only. Organizations that fail to address global threats will find themselves at a competitive disadvantage and fall victim to ever more technologically sophisticated criminals.

In conclusion, sophisticated and global governance challenges can be addressed only by sophisticated and global governance tools and methodologies, and this is where MASTER integrated project comes in picture.

OBJECTIVES OF “MASTER” PROJECT

Master (which stands for Managing Assurance, Security and Trust for Services) is a European Commission project inside the FP7, which is the short name for the Seventh Framework Programme for Research and Technological Development. This is the EU's main instrument for funding research in Europe and it will run from 2007-2013. The Master project consortium includes major industry players such as Atos Origin (ES), SAP AG (DE), Engineering (IT), British Telecom (UK), IBM (CH), ANECT (CZ) and Deloitte (FR), as well as a number of academic partners and end-users: Lero (IE), University of Trento (IT), ETH (CH), University of Stuttgart (DE), SINTEF ICT (NO), CESCE (ES) and Hospital San Raffaele (IT).

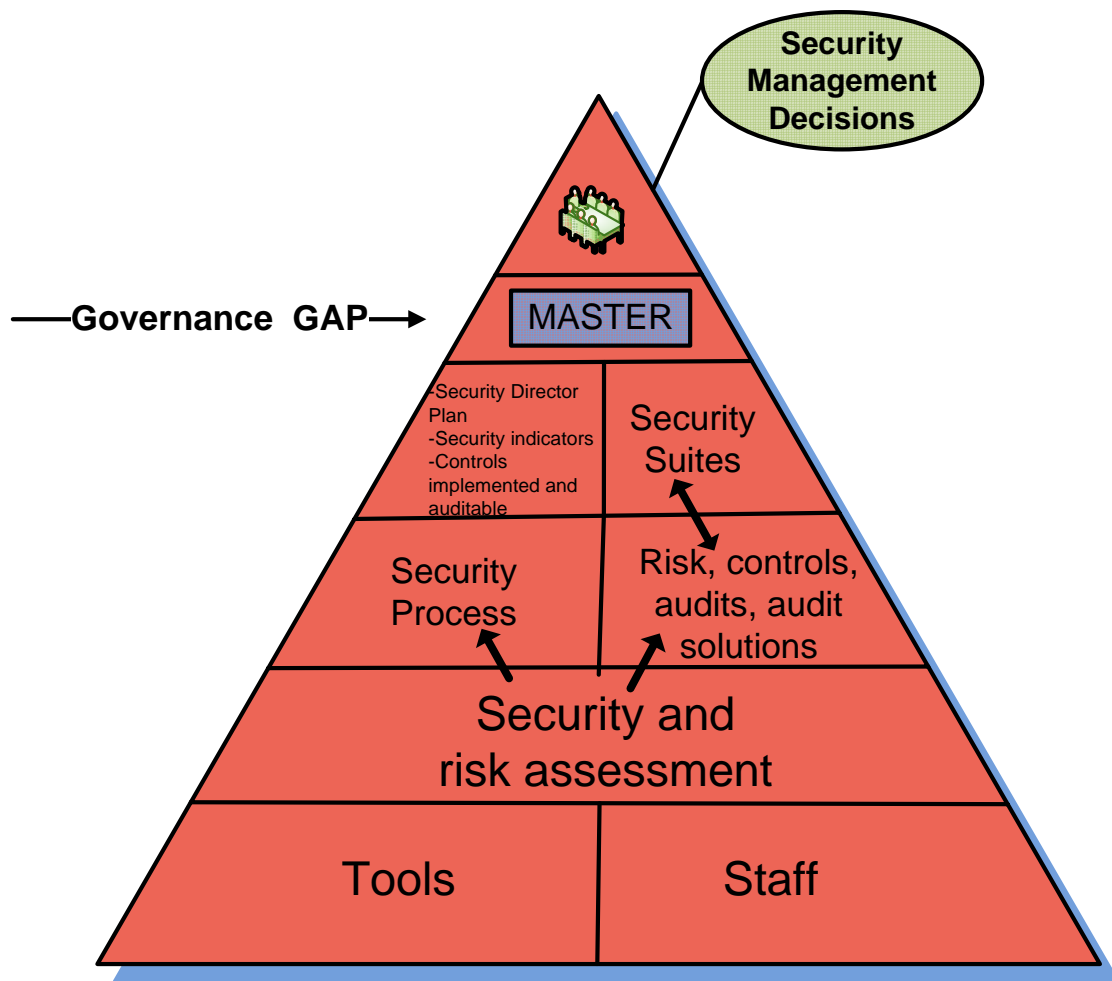
This research and development project has a 15M Euros budget and three years of work, starting from February 2008, in order to provide methodologies and tools that facilitate monitoring, enforcing, and auditing quantifiable metrics of the security of a business process, with a special focus on regulatory compliance in a highly dynamic service- oriented architecture. All of this is going to be implemented, tested and validated in three different types of business relation settings and governance models: centralized, distributed partnerships (multi-domain), and outsourcing contexts.

The first project step is a risk analysis of the different process parts in which Master system infrastructure elements have to be integrated. This approach covers the security requirements coming from the different Governance Levels (Business, ICT and Security level). The second step is the creation of a “universal” language that models all the security requirements extracted and defined in the previous step. Transforming these common and “observable” security requirements in a language that upper automation level understands is a key issue that is likely to affect the overall success of MASTER solution. The following project research directions are related to extraction of the information from the different levels of the organization (process, IT infrastructure...) with Master monitoring architecture,

consolidation of this information with the security requirements and a real-time dashboard that contains the security indicators for the processes observed. Finally, the last and one of the most important research directions in Master is optimisation and automation of the Assessment and Enforcement infrastructure. Architectural components in these infrastructures are based on techniques and tools for analyzing events produced by the MASTER monitoring infrastructure in order to perform detection of policy violations, analyse and understand causes of policy violations, derive and predict models for violations, perform compliance analysis etc.

When it comes to governance alignment and the (semi)-automated control of Governance objective achievements, the most important aspects are related to the establishment and mapping of right metrics across levels, selection of the best practises and indicators, as well as the Governance “impact” model with a weight assignation to the process compliance model, the percentage and distribution of implementation inside the global organization etc. The indicators selection will help in the definition of goals and objectives that the Master methodology must fulfil. In our case Key Goal Indicators (KGI) establish measurable business objectives that must be reached to obtain successful services, whereas Key Performance Indicators (KPI) set up the measures on the business or technological infrastructure (such as the number of “negative” events) that allow to evaluate the level of goal achievement. In this sense, the Master will improve the current state of the art related to the Information Security Governance through a consistent approach for mapping indicators (KPI and KGI) from high level business objectives, processes to low level controls, while setting up a flexible and efficient framework to measure and assure security and compliance levels in an organization.

The figure below explains the positioning of MASTER in respect to the related security tools, processes and stakeholders.



While at the bottom of the pyramid, we usually have low level security controls (performed by software tools or manually by staff) that are tightly coupled with the actual organisational and ICT infrastructure, upper technical and non-technical assessments, as well as security processes, audits, integrated controls etc, can be more loosely coupled both in horizontal and vertical direction. Recently we have witnessed appearance of the first “high-level integrated governance solutions” often based on previous work in security compliance checking, monitoring infrastructures or risk assessment tools. However, no matter how sophisticated these integrated tools go, the promise of complete security governance will always remain that: a promise. The human intervention will always remain at the top of governance pyramid, although Master project, once it delivers its results, is hopefully going to minimize these interventions.

REFERENCES:

[1] IT Governance Institute, Information Security Governance Guidance for Boards of Directors and Executive Management, 2nd Edition, 2007

[2] Atos Origin and NCC Report on Security and Information Risk Survey, www.atosorigin.com

[3] Atos Origin Research Report, Tackling Compliance to Reap Long-Term Benefit, Research report, www.atosorigin.com

[4] Julia H. Allen, Jody R. Westby, *Governing for Enterprise Security (GES)*, February 2007

[5] Business Software Alliance, 'Information Security Governance: Toward a Framework for Action', 2003

[6] Hallawell, Arabella; Gartner Global Security and Privacy Best Practices, Gartner Analyst Reports, 2004

[7] IBM, Data Governance Council, *Oversight of Information Security*, 2005

[8] Moulton, Rolf; Robert Coles; 'Applying Information Security Governance', *Computers and Security*, Elsevier Ltd., 2003