Functional Security Model: A Way to Link Technological Affairs with Companies Management

Edward Paul Guillén, Rulfo Quintero

***Abstract*— The information security not only has become a relevant business subject but also a complex decision topic for non-technical people. Legal framework, monitoring security, best practices, standards compliance are part of the security solutions but they can become in the principal complexity affair. This paper shows a general security overview to converge in an initial functional security model in order to achieve a complete solution. The preliminary approach tries to give tools for experts and non-experts managers and let them easily to understand and to apply a solid security framework.**

***Index Terms*— Security Models, Management. Web technologies. Security platforms**

I. Introduction

Nowadays information security is more relevant for organizations than ever before and because of the legislation compliance, some medium-sized and international companies already have been started to working on it, but it is important that everybody tries to do it. In fact, strategic security suggests to apply and to recognize the informatics security as a key business component which must be present, and proactively adopted inside all company levels and departments. To achieve this, tools and mechanisms are required in order to plan, to execute and monitoring a functional model. For small industries it is very important to optimize resources, and it has been proved to be more efficient under better planning environments. To analyze the strategic security as a company's necessity in order to link the technological details and their complexity with the people who take the economical decisions, we will present a legal framework with a group of lesson learned with SOX experiences and after that we will give a security definition from a strategic function approach. Then, we will show some functions to be implemented in a model like monitoring and outsourcing. Finally, we will try to propose the steps to implement a functional security model with online wizards, keeping in mind standardized models and similar experiences.

Manuscript received July 22, 2007. E. G. Author is with the Military University "Nueva Granada", Bogota, Colombia (phone: 571-6862693; fax: 571-5665720; e-mail: edward.guillen@umng.edu.co).
R. Q. Author is with the Military University "Nueva Granada", Bogota, Colombia (phone:571-6862693; fax: 571-6862693; e-mail: gissic@umng.edu.co).

II. Legal Frameworks Influence

Most of the people think that information security is a relevant subject only for engineers and security architects inside an organization. Nevertheless, security goes beyond technical resources, operators, security tools, and indeed it includes a cooperative technical, operative and management effort that relates the whole organization through controls application and security policies implementation.

Security is an evolving area which in its beginnings was not regulated by law. But due to transparency problems, cyber terrorism, online business, partners and stakeholders connectivity, it was necessary a strong legislation development like HIPAA (The Health Insurance Portability and Accountability Act, which covers privacy rules for people handling healthcare information), SOX (Management's assessment of internal control over financial reporting), GLBA (The Gramm-Leach-Bliley Act, which describes privacy protection rules for the banking and financial services industry), COPA (The Children's Online Protection Act, which covers a broad area of information access and protection for children), and others, which has been the triggers to start to work in the security field across the entire organizations.

When SOX was released, it was not expected that IT staff would be so important to be SOX compliant, but when statistics showed that 70% of time was used to solve deficiencies on IT controls, and 70% of the security budget was spent identifying the rights controls to apply on IT, the subject became really relevant [3]. And by the other side the numbers revealed a very expensive and inefficient first years of work to be SOX compliant.

Companies are trying to apply too many IT controls during these first SOX years, without selecting them carefully. The security designers should have in mind the multidisciplinary essence of the security with special emphasis in the active management participation and in the realization of educational programs.

Due to language between management and engineering is so different, it is very important that engineers recognize management concepts like risk management as managers the security concepts, then we can put them inside an unified framework to join efforts to fulfill a complete strategic security.

III. LESSONS LEARNED FROM SOX

It is very significant to identify the right way to motivate all people belonging to the organization, to commit with regulation compliance. Next, we will show five related factors that were analyzed by security researchers in North American experiences [3].

1) Deliver continuous training to employees while ensuring accountability with policy: Being strategic and relate everybody inside the organization is more likely to achieve and maintain compliance.
2) Restructure the risk management function, internal controls, and IT security: risk involves integrate multiple disciplines and departments across organization. Experience shows that many resources were used to solve IT security controls deficiencies, policies, procedures and their management.
3) Reallocate IT expenditures by shifting spending from consultants and contract labour to automated tools: The control deficiencies decrease as the company increase the investment on IT security. In the other hand it was revealed that is more useful invest on automated IT based continuous control and monitoring tools, than on contractors and services.
4) Automate IT measurements, reporting, controls, change management processes, and IT security policies: focused on documenting procedures, making changes to both business and technical procedures, and automating these processes as much as possible.
5) Focus on managing risk to improve IT controls, information collection, and reporting.

TABLE 1: RESPONSIBILITIES DISTRIBUTION AS A RESULT OF LESSONS LEARNED.

Lesson No.	CEO	Admin. IT	Internal Auditor	Corporative legal
1	X			X
2	X	X	X	
3		X		
4		X	X	X
5	X	X	X	X

The suggested responsibilities distribution between the different roles inside any organization is shown on Table 1.

The most successful applying control to be SOX compliant where companies which invested to identify the IT controls needed to satisfy SOX and then put procedures and tools in place to monitor, automate, and report on these controls.

There is an emerging issue: "data custody", which involves data protection, data privacy, data retention, data destruction, and data discovery. The research shows that custody of sensitive data was more important for many organizations in the last 12 months. Because most of this information resides on IT systems, “the question of general IT controls and information security controls designed to safeguard sensitive data has come to the forefront” [3].

IV. SECURITY AS A STRATEGIC FUNCTION

It is very clear that this issue goes further technical implementations, and it means to think in a whole process integrated into the core business function, where find the right reporting structure for security is between looking at it as an information technology function or as a control function.

Security is an evolving area, and learning while it evolves is important for executive managers.

This commitment is wrote in mission statements and transfers this ideals internally and to their customers, as the results of applying strategic information security models, and giving trust to other companies as a good business partner.

Information security strategic role understanding must include at least the next basic rules:

1) Information is an asset that is critical to the success of the business. As a result, the information assets of the company must be protected against relevant risks.
2) Information security must be integrated with business plans.
3) Customers should expect that the company will respect their privacy and protect their information with the same diligence that will be used to protect its own information.

It is important to understand the necessity of safeguard the information in nowadays global interconnected market. To achieve this change are important the next steps.

1) Made a deep understand of the problem and the risks a business faces
2) Use the correct steps to mitigate those risks.
3) Measure the success of the security program and monitor it to ensure that it continues to function at the desired level.

All CIOs need to know security reasons based on information triad CIA (Confidentiality, Integrity and Availability), and more detailed Parkerian Hexad (Confidentiality, Possession or Control, Integrity, Authenticity, Availability and Utility). This concept helps him to understand the global implications of security in organization behaviour, specially its business core.

Information security professionals point of view is a further definition of CIA and Parkerian Hexad, to accomplish this CIOs support on CBK (Common Body of Knowledge), COBIT, ISO 27001:27005, OSSTMN, SDL, best practices, and others security frameworks and guidance documents that have been integrated to security and are operated, sometimes from similar point of view and others from a complementary one.

The next example shows the different points of view about a new service deployment, when business man and security agent meet to talk about it. a) For business man, whom technical things are easy and ROI (Return of Investment) and cost effective solutions important. b) Information security professional will be focused on solutions, product features, and implementation issues. Therefore his conversation will be reflected on many technical questions of huge importance.

The conclusion in this well known circumstance inside any organization, is the importance of keep in mind both of them, and create a life cycle approach of information assurance, to a solution that will be good for both of them: business and

engineering. Putting together both technical and business view is essential to move security into a strategic role.

CEOs are familiar with risk management and this is an important advantage, because security behaves in a similar way and they don't need to know about the technology to face risk management. However they will be careful to who delegate such responsibilities given that CIO use to be 2 levels down, giving the impression that security is less important.

"The business manager will set lofty goals and have challenging aspirations. The security manager must learn that those goals are his goals too, but his job is to ensure the goals are met with a minimum of risk. That is the real challenge of defining strategic security" [1].

V. STRATEGIC SECURITY MONITORING

Strategic security depends of monitoring of its strategy to succeed. A Proactive, flexible, updated, documented strategy, which tests constantly the new rules to react to novel challenges and deploying the computer security incident response team CSIRT (outsourced or not), with policies, procedures and escalation plans to communicate with management, are a must.

This will be monitored proactively in the form of Security Information Management (SIM) products which runs a console to analyze information and agents to recollect it in all the devices to be monitored, It is clear that monitoring is beyond a single product. It is a hard work take one of these products and adapts it to internal policies, but It is very important too.

Information security management can be achieved in three ways:

1) Using existing tools for monitoring and reporting in consoles, like HP OpenView http://h20229.www2.hp.com/ and IBM Tivoli http://www-306.ibm.com/software/tivoli/.
2) Consolidating information through product consoles. It is more possible since multi-function appliances appearance. According to Gartner, an appliance is "a computing entity that delivers predefined service(s) through an application-specific interface, with no accessible operating software" [2].
3) Implementing a **S**ecurity **I**nformation **M**anagement –SIM– product: This approach is in theory the best solution, it deals with diversity to do correlation, but It is the most expensive.

It is highly recommended open and secure standards usage, which reduce the likelihood of monopolies and transparency doubts inside security platforms, on processes such as data gathering, monitoring, management, unified storage, correlation and presentation.

VI. OUTSORCING SECURITY FUNCTIONS

When enterprises thought on outsourcing, usually it is associated with the necessity of reducing operational (staff) and acquisition costs (technology), looking for a bigger ROI, and trying to transfer some responsibilities to the service provider.

However, it could be about sign with more specialized security companies and understand the agreement terms, and the kind of offered services such as operations, monitoring, design, management, decision making with or without value-add.

Any third party will not only being protecting, monitoring and comply with policies and requirements but this service provider has the potential to handling, analyzing, exposing, thieving and even selling company's more sensitive information.

Experiences report, the best equilibrium is reached when organization IT personal guides the service provider inside unique organization characteristics and eventually, the provider drives his work aligned with organization objectives.

VII. A FUNCTIONAL SECURITY MODEL

In the security World, there are documents which guide organizations from diverse point of view to get a better security level from management to daily operations. However these documents are so extensive that organizations use to lose their goal. A functional security model suggests being a practical help to work with this documents.

IT security professionals have read the CSI and FBI security reports (http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml) which report security behaviour during the year. But W. Baker y L. Wallace show that the way surveys questions are done, are not the best kind of question to extract more valuable information of their participants therefore this report cannot show more realistic information [4].

Including such tips inside a functional security model, it is shown that recollect and associate information is not enough and the necessity of design better strategies to react to security challenges is more relevant because this can affect their applicability results.

Fig 1 shows the proposed functional security model. This model integrates and put in its strategic place some of the most effective methodologies and frameworks as a quick guide inside the IT and security management world.

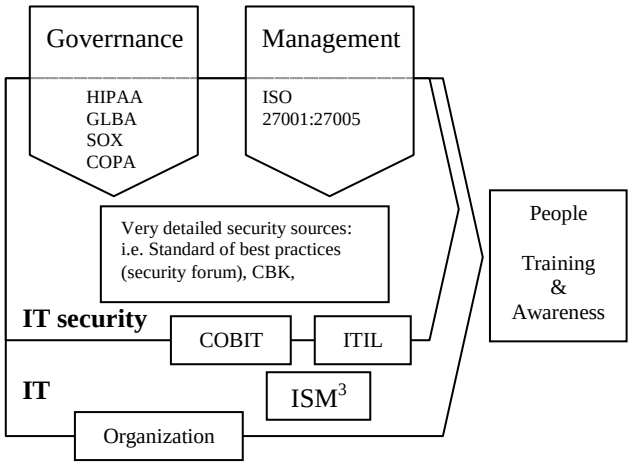

FIG 1 FUNCTIONAL SECURITY MODEL

IT governance and management related with IT security operations, can't work without IT itself so COBIT and ITIL support IT at the organization and ISM3 represents the quality vector.

Finally, people require continuous training and awareness plans for day to day operations against new and ever changing threats, in this field creative ways to work with groups are highly recommended, it doesn't matter how difficult a subject could be as shows COBIT training program at www.cobitgames.com.

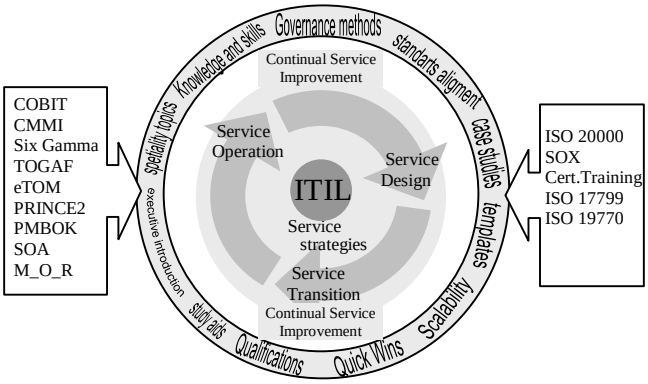

FIG 2: ITIL 3 DIAGRAM

A. *ITIL 3.0 useful guidelines*

Few years later ITIL 3 has a new face as shown on Fig 2, and a new way to see services implementation and enhancement focused on a comprehensive IT-Business alignment. Compared with ITIL 2, it is notorious how the security component has been integrated with many others without any kind of differentiation, for simplicity, and assimilation of the security importance by ITIL experts as a strategy of many interactions and implementation of best practices guidelines [5]. Therefore ITIL is other good example about management trends, innovative and strategic cyclic process and best practices utilization.

VIII. IMPLEMENTING A FUNCTIONAL SECURITY MODEL

A. *The First Security Step*

The first step is to get a copy of SOX, COBIT, ISM3 which extends ISO 9001 quality management principles to information security management (ISM) systems and is distributed under Creative Commons license, and CBK (if available), because CBK aims to reconcile industry and academia needs and reflect information security's multidisciplinary nature [6], as starting IT security frameworks, and other important documents like manufactures guidelines as shown on Fig 3 without forget its unique strategic position and scope.

Maintain the idea that any organization has some kind of policies, even written or not, applied or not, and start with an audit to determine the initial conditions of the organization, in a first stage, considering all IT targets as black box and lately as a white box.

The next step is to Document, catalogue and centralize the audit results in a corporative portal under a restricted area protected for any authentication mechanism. This process allows the group to develop a self assessment and found the key security controls and even more general IT controls. The GISSIC ethical hackers did the audits and used the portal http://gissic.umng.edu.co to handle all the resulting information.

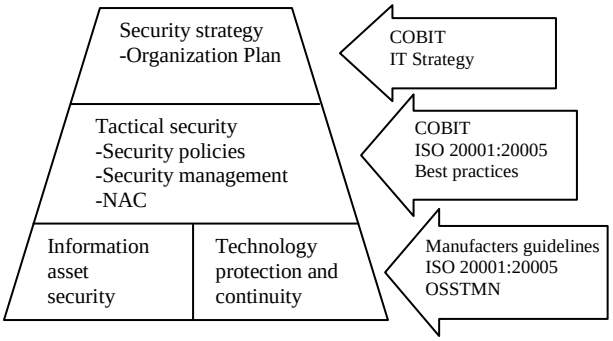

FIG 3: GUIDES AND THEIR STRATEGIC SCOPE

The risk could be identified if the vulnerabilities identification is made in an early stage with information that must be real and potentially manipulated. In that way, key controls can be easily identified and applied, optimizing resources and effort in the planning and execution of tasks.

A remarkable point is about web technologies. As stats suggest, the web is the first target of 2007. GISSIC research security group is developing data-mining techniques to correlate all risks events, thinking in a preventive and proactive approach against insiders with the capability of use search engines with hacking purposes. With this information, it will be possible to create risk profiles per web user, and determine criminal profiles and take isolating and quarantine countermeasures against potential high risks and suspicious activities.

B. *Management Communication Channels Importance*

The collected information must be shown in easy terms to management. This will support the key finding of IT security deficiencies on technology, training, processes, policies, management and decision making areas. Communicative skills are a must for security team, as previously shown in section 3.0 Strategic security.

Cyclic security model is shown on FIG 4, as a continuous plan, do, check, act to enhance the team level while more experience is acquired. This only can be achieved relating people belonging to different areas, with different roles and management points of view of security, privacy and business continuity to help in the policies creation process and daily applicability.

C. *Work Plan Importance*

As a result of information analysis, we suggest a working

plan based on open source software which characterize for reduce acquisition costs, increase flexibility, dynamism, information sharing and even enhance security under certain circumstances compared with closed source developing model [7],[8]. Open source tools include: risk management, project management, knowledge base, bugs tracking, control tools, massive training channels, policies and strategic plans organization facilities for multidisciplinary teams.

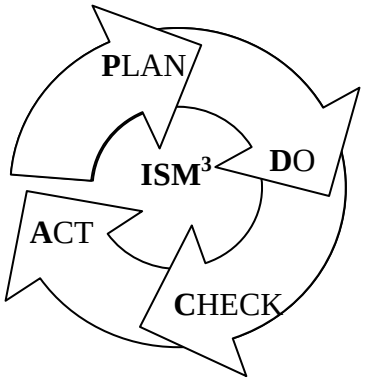

FIG 4 CONTINUOUS CYCLIC PROCESS PHASES

D. Involve Suppliers In The Process

In a functional security model application, it is clear that decisions done by the organization must be implemented not only internally but in the whole production chain. If some deficiencies directly related with the core of the business on suppliers resources are found, the group suggest that third party uses some automated methodologies like OWASP Top Ten Project [13] or Automated Security Functional Testing (NIST) [14], to solve this deficiencies together

E. Using Open Source Tools

During acquisition process, measuring advantages of open source software and determining more pros than cons, GISSIC group is using open source software tools with reporting capabilities for monitoring, like the promising Cobia, its Strata IPS and OSSIM, which are fundamentals to keep control and think in adaptability, flexibility and governance as a reachable challenge on real time [9].

Some solutions and appliances [10] which simplify monitoring and integrate multiple protection mechanism with enterprise quality, does not fit neither to security policies nor attack prevention strategies on some organizations. There are projects that try to integrate tools under unified and adaptable platforms, which by definition must be open to do not monopolize and constraint the final result. One of this security platforms is called HEKA, a Military University "Nueva Granada" open source project for designing security modules, for adapting them to organization necessities and focused on functional security [11],[12].

IX. FUNCTIONAL SECURITY MODEL WIZARDS

This research has been materialized into web wizard modules that guide users into security questions. These wizards help CEOs (Chief executive officer), CIOs (Chief information officer), and CISOs (chief information security officer), in the large process of being compliant with some legislation at many levels of the organization, in a self explanatory vocabulary and inner skills for each created wizard role.

Wizard's modules have been catalogued in the next domains, inspired on CBK for the reasons explained above:

1) Access control and methodology
2) Telecommunications Network and Internet Security
3) Security Management Practices
4) Applications and systems development security
5) Cryptography
6) Security Architecture and Models
7) Operations Security
8) Business continuity planning (BCP) and disaster recovery planning (DRP)
9) Law, Investigations and Ethics
10) Physical Security

Wizards have report interfaces and its outputs can be shown on management and decision making people meetings to show results and levels of IT security and resolve differences obtained on wizard answers and actual policies statements, to update and adapt policies and procedures into more realistic and effective ones.

During our beta tests, it has been very interesting find incoherencies on the wizard results, between CEOs, CIOs and CISOs mind to the questions. And often it is directly related with holes in policies and poor communication between all of them. These communication problems have been reduced after data recollection and these have been communicated to the participants as a feedback capability of the model and platform implementation.

X. CONCLUSIONS

Asynchronous and collaborative wizards and portals enhance and take advantage of people available time into the organization, and well designed graphical wizards with different roles and questions capabilities can set a common starting point for management, IT groups and security experts in the way to identify the security weaknesses and implementation methodologies.

Although a wide variety of security models have been proposed, the election of one of them is a matter of experience, education and application. The experts decide but moving away the knowledge of most people at the companies because of their specialized concept. However it is possible to propose software based wizard that helps the inexpert management to achieve a reasonable security level according to the company security policies.

The functional security model characteristics demand to involve the whole company process according to the designed security policies. Even the suppliers and their processes must be followed.

After the model has been designed, the application must be deployed by using open source software tools with security platforms to achieve a distributable and integral

software-hardware solution. However the monitoring not only covers the technological solution but also the human security weaknesses.

REFERENCES

[1] J. Wylder, Strategic Information Security Auerbach Publications, 2004.
[2] N. MacDonald, T. Bittman, M. Reynolds, B. Gammage. "Findings: Not all appliances are appliances". Gartner. White paper, September 2006.
[3] Symantec Corporation. "Lessons Learned for SOX Compliance and Other Regulatory Challenges". White paper, May 2007.
[4] W. Baker, L. Wallace "Is Information Security Under Control? Investigating Quality in Information Security Management". IEEE Security and Privacy, Vol. 5 No. 1, February 2007, pp. 36-44.
[5] B. Clacy, B. Jennings "Service Management: Driving the Future of IT". IEEE Computer, Vol. 40 No. 6, May 2007, pp. 98-100.
[6] M. Theoharidou, D. Gritzalis. Common Body of Knowledge for Information Security". IEEE Security and Privacy, Vol. 5 No. 2, April 2007, pp. 64-67.
[7] Trend Micro: Open source is more secure. Available: http://news.zdnet.com/2100-1009_22-6083490.html and http://news.zdnet.co.uk/security/0,1000000189,39274646,00.htm
[8] Why Open Source Software / Free Software (OSS/FS, FLOSS, or FOSS)? Look at the Numbers! Available: http://www.dwheeler.com/oss_fs_why.html
[9] L. Herreros. "NAC y Gestión de Vulnerabilidades. Desarrollo de Negocio-Área de Seguridad". Sociedad de la información. February 2007. Available: www.socinfo.info/contenidos/pdf34feb07/p12-34datos.pdf
[10] Sophos. " Managed appliances, security solutions that do more". White paper, May 2007. Available: http://whitepapers.zdnet.co.uk/0,1000000651,260281023p,00.htm
[11] E. Guillén, J. Constante, M. Hernandez. "Self-Management Security Design Platform HEKA". Proceedings of Mexican Conference on Informatics Security 2006
[12] E. Guillén, R. Quintero. "Hacia un modelo de seguridad funcional: casos prácticos que sugieren su utilización". Proceedings del Simposio Internacional de Tecnologías de Información y Comunicaciones- TIC. March 2007.
[13] Owas top ten Project, available: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[14] Automated Security Functional Testing (NIST) Project, available: http://csrc.nist.gov/auto-func-test/index.html