International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.111-120
http://dx.doi.org/10.14257/ijsia.2016.10.3.10

Holistic Performance Model for Cyber Security Implementation Frameworks

Issa Atoum[1] and Ahmed Otoom[2]

[1]*Faculty of Information Technology, The World Islamic Sciences & Education University, 11947 Amman, Jordan*
[2]*Royal Jordanian Air Forces,11134 Amman, Jordan*
[1]*Issa.Atoum@wise.edu.jo*
[2]*aotoom@rjaf.mil.jo*

Abstract

The performance measurement process identifies if an implementation process is within acceptable thresholds. Performance measures for cyber security implementation frameworks are considered strategic controls because it can guide the implementation process. Consequently, corrective or predictive actions could be applied to resolve a security issue early in the implementation process. However, to our knowledge, there are no performance measures designed to function at the country level for cyber security implementation frameworks. As a result, cyber security strategy implementation process is left uncontrolled. To resolve this issue, this article proposes a new holistic performance model that is based on the well-known balanced scorecard. It aggregates performance measures from various entities involved in executing cyber security strategies. The inception of the proposed model draws its applicability to address performance measurement of holistic cyber security implementation frameworks.

Keywords*: Cyber Security Implementation Frameworks, Performance Measurement, Balanced Scorecard*

1. Introduction

The goal of cyber security performance measurement is to quantify values about services and processes during service execution. Thus, the security authority could identify if current actions being taken are within acceptable thresholds. Consequently, corrective actions could be applied. An acceptable security measurement technique (from the upper management viewpoint) should make stability between financial and non-financial measures. Moreover, it should allow measurement of the security achievements at the country (national) level [1], [2] rather than departments or organizations levels. To our knowledge, there are several frameworks and techniques that can be used for performance measurement [2]. Traditional approaches such Return on Security Investment (ROSI) and Annual Loss Expectancy (ALE) do not suite security because it is hard to determine the value of security investment versus returns. It is known that a security incident can affect reputation, or even be catastrophic (*e.g*. Stuxnet worm [3]). Therefore, a suitable performance measure should take care of measurement strategically and aligned with the country business goals. One dimensional performance measures cannot give the full picture of performance due to its being favored toward one performance aspect such as financial aspect while not considering other aspects such as customer, or risk aspects. Nowadays financial and non-financial performance measures are considered major milestones for security systems.

Cyber security strategy provides long plans for the cyberspace (*e.g*. [4], [5]). Thus, it is likely that the execution of such a strategy will take several years. Consequently, each

ISSN: 1738-9976 IJSIA

goal may take long time to get results of lagging indicators. Hence, a suitable measure should work at the national level exploiting the business and financial needs. Recent works showed that the performance measurement is considered a Strategic Control (*i.e*. component) for cyber security frameworks [6][7]. To develop this component, we suggest exploiting an approach based on the Balanced Scorecard (BSC). The BSC is a strategic planning and performance measurement technique used widely by commercial companies, governments, and non-profit organizations. The major advantage of the BSC is that it can align business activities to its planned strategies [8]. The BSC has variant models. The model of Norton and Kaplan[8] has four perspectives: Financial, Customer, Internal Business Process and Growth perspectives[9]–[12]. Each perspective is assigned a list of performance measures to assist in calculating the cumulative performance of a strategy during its implementation.

The BSC is a good choice for performance management due to many reasons: 1) the high usage of such a framework worldwide. According to Bain & Company reports, the BSC is being used internationally in more than 63% of worldwide entities [13], and 2) "It is distinct from other strategic measurement systems in that it contains outcome measures and the performance drivers of outcomes, linked together in cause-and-effect relationships" [14, p. 67] .

Although the BSC was used originally for business it has been modified for IT use [15]. Herath *et al.* [16] modified the BSC to be used for information security frameworks. This makes it a useful enabler component in cyber security implementation frameworks. We borrow Herath *et al.* [16] model and modify it to work at the national level. We call the new enhanced BSC, a Holistic IT Security Balanced Scorecard (H-ITsec-BSC). The H-ITsec-BSC enables the cyber security implementation framework to manage, monitor, and control performance on a national level. The proposed model aggregates the performance state from all involved entities executing cyber security initiatives. The H-ITsec-BSC is based on adding an additional level over the ITsec-BSC level. The new level links the strategies with goals and sub goals. It monitors the performance globally during the execution of cyber security strategies.

First, we discuss related works. Next, we illustrate basic concepts of the Information Security Balanced Scorecard. Then, we discuss the proposed model. Finally, we evaluate the proposed model and conclude this article.

2. Related Work

According to [17] more than 3,600 articles in performance measures have been published between 1994 to 1996, which then was described as a revolution. Taticchi [18] showed that the Performance Measurement and Management (PMM) has notably increased in the last 20 years. Thus, literature showed many performance measures models and framework in various domains [1], [2].

However, good cyber security performance measurement techniques should balance between financial and non-financial measures, and they should allow measurement of the security achievements at the national level. Cyber security strategy implementations should also have a performance measurement to control the performance during implementation [7]. The nearest performance measure to our work is the BSC [8]–[12] [16]. The BSC is commonly used in service and quality management [15], [19]–[22]. Herath *et al.* [16] modified the Kaplan version[8] of BSC to measure security of an organization.

3. Information Technology Security Balanced Scorecard

Herath *et al.* [16] have modified the BSC of Kaplan[8] to be used for information security frameworks. Herath's BSC is named (ITsec BSC). The ITsecBSC consists of four components:

- The Business Value Perspective: The major concern of information security is ensuring protection of information against loss, disclosure, damage or disruption. This perspective covers the security principles such as Confidentiality, Integrity and Availability. Therefore, this perspective aligns with our concern of cyber security implementation frameworks goals.
- Stakeholder Orientation Perspective: Ensuring that desperately stakeholder needs, behaviours, actions are taken into consideration for information security. Cyber security implementation frameworks incorporates communications with various stakeholders ranging from workers, users, managers, customers and even third party entities. Thus, this perspective aligns with cyber security implementation frameworks in terms of diverse stakeholders' involvements.
- Internal Process Perspective: The set of actions, and procedures that are followed in the organization to ensure security. The cyber security implementation frameworks has a set of policies, processes and other components that need to be carried out towards achieving cyber security. So, this perspective aligns with our intention in cyber security implementation frameworks.
- Future Readiness Perspective: Threats are constantly evolving and thus there should be a future thinking of expected threats, thus planning and acting against them. This could be achieved through the acquirement of new technology, tools, and preparing security professionals for new challenges. The cyber security implementation frameworks has a set of controls including: Awareness, Vigilance, Capability Building, Risk Management, Quality and other controls that align with this perspective. Therefore, this perspective aligns with our intention in cyber security implementation frameworks.

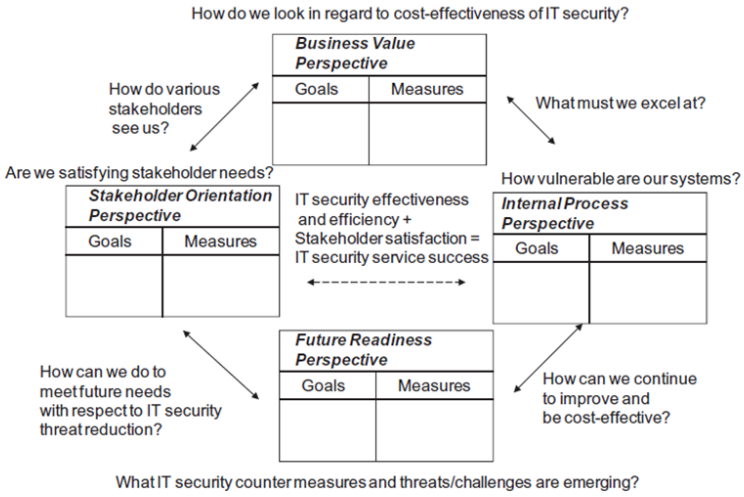

Figure 1. ITsec BSC Model [16]

4. Proposed Model

Figure 1 shows the ITsec-BSC model. It has several drawbacks. It is built for the level of an organization and below. Moreover, the BSC is "seen as myopic and ignores the activities and initiatives that goes beyond the original targets" [23]. Furthermore, the BSC can point out problems but not how to reveal them [24].

A suitable performance measure should tackle cyber security strategy execution that might take several years. Each cyber security goal may take long time to get results of lagging indicators. In other words, the strategy map/dashboard will be idle for long time and decision makers cannot take actions with no available information. Consequently, many problems may arise from the adoption of non holistic performance measures (such

as BSC in as “as is” basis). Subsequently, the cyber security implementation frameworks will not be able to track the cause of the degraded performance unless a suitable holistic performance measure is enabled.

We propose an enhancement to Herth’s ITsec-BSC to make it fit for the cyber security implementation frameworks needs holistically. We call the new enhanced BSC, a Holistic IT Security Balanced Scorecard (H-ITsec-BSC). The H-ITsec-BSC enables the cyber security implementation frameworks to manage, monitor, and control performance on a national level. It aggregates the performance state from all involved entities (various related organizations) executing cyber security initiatives. The cyber security strategy (CSS) implementation involves government entities, the private sector, and even the citizens. While the H-ITsec-BSC will be used for various organizations and private sector companies. Usually related organizations will hide details of their performance measures (*e.g.* BSC) and only expose a small portion of their BSC to related entities for privacy reasons. An exception is that the relevance of these details is mandated by law and or regulations. Moreover, each organization has its own goals which may be subset or parallel to the CSS implementation goals. For example, an Internet Service Provider (ISP) might have initiatives to enhance customer services, and at the same time have a mandatory role to execute one of the national CSS objectives such as protecting national internet gateways.

The H-ITsec-BSC is linked to entities to be able to provide the required overarching view or holistic performance. This link can be implemented by exploiting the primary/foreign key concepts used in the relational data models. A primary goal on the holistic level may be satisfied via achieving one or more than one sub goal by the participating entities. With this link to the involved entities, we can track who is doing what, and therefore managers will be able to take corrective actions. In other words, if a goal leading indicator is degraded then managers, can know who is responsible for such low performance and actions can be taken holistically.

Figure 2 shows the proposed model. Each participating entity is running its own version of BSC, and possibly other performance measurement techniques. Each entity performs its own part in implementing CSS goals. The H-ITsec-BSC enables measurement at the national level. It aggregates results from various participating entities and links the sub goals to the CSS major goals. The aggregation can be a weighted average, summation, or any other suitable algorithm selected by the Cyber Security Authority (CSA) as deemed necessary. The aggregation process must be configurable and allows using different algorithms to aggregate data for different goals. For example, the awareness and capability building goal of CSS might have several sub goals being executed by different entities; national TV will run an awareness campaign for citizens, a security company will train professionals on how to prevent email attacks, another campaign will be conducted online to get e-commerce users be aware on how to prevent credit card frauds, *etc*. Our proposed Holistic BSC helps in solving the problems pointed out by [24] and [23].

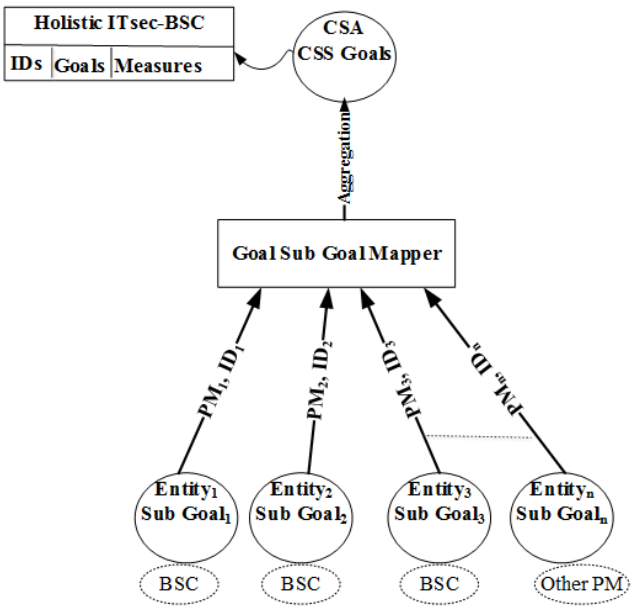

Figure 2. Proposed Model

4.1 Formal Definition

We formally define the holistic performance measurement process as follows: given a set of goals in the CSS document.

$\boldsymbol{G}$ = { g_1, g_2, …,g_n }. A set of Entities $\boldsymbol{ENT}$ = { ent_1, ent_2, …,ent_h}. Each Entity has a performance measure $\boldsymbol{PM}$ = {pm_1, pm_2, pm_3, .., pm_x } for each sub goal . Then we define the following formulas:

List of sub goals for a goal $\boldsymbol{G_k}$:

$$\boldsymbol{sub_{goals}(G_k) = \{G_k Sg_i\}, \forall i = 1, m} \quad (1)$$

where:
$\boldsymbol{G_k}$ is any goal $\in \boldsymbol{G}$.
$\boldsymbol{Sg_i}$ is any sub goal $\boldsymbol{i}$ of goal $\boldsymbol{G_k}$
$\boldsymbol{m}$ is number of sub goals of goal $\boldsymbol{G_k}$

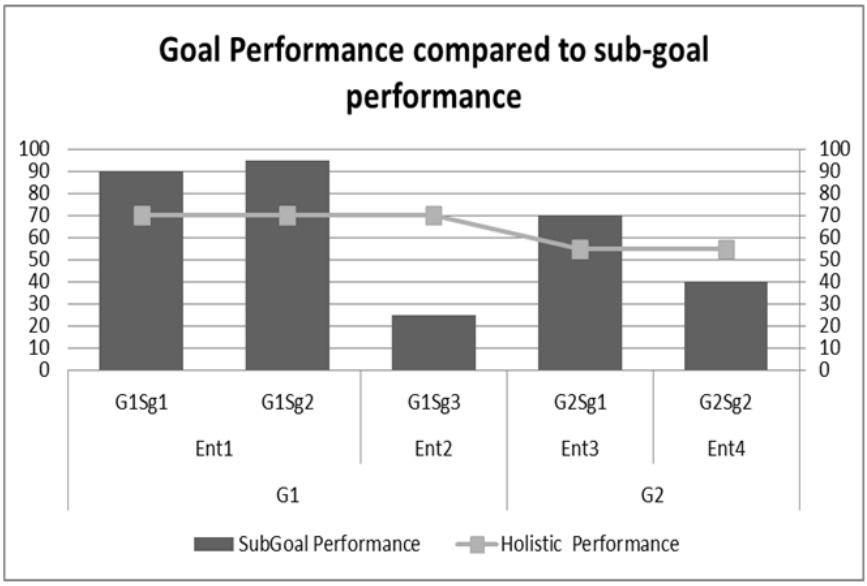

Figure 3. Goal Performance Compared to Sub goal Performance

The formula (1) links all goals with their respective sub goals, such that all performance metrics related to one goal will be linked with all its sub goals.

Then, the performance measures of any sub goal are defined using:

$$Sub\_goal_{performance}(ENT_j, Sg_i) = PM_i \quad (2)$$

where:

ENT_j is any entity $\in ENT$

Sg_i is any sub goal i as in formula (1)

PM_i is the performance of any entity j on sub goal i

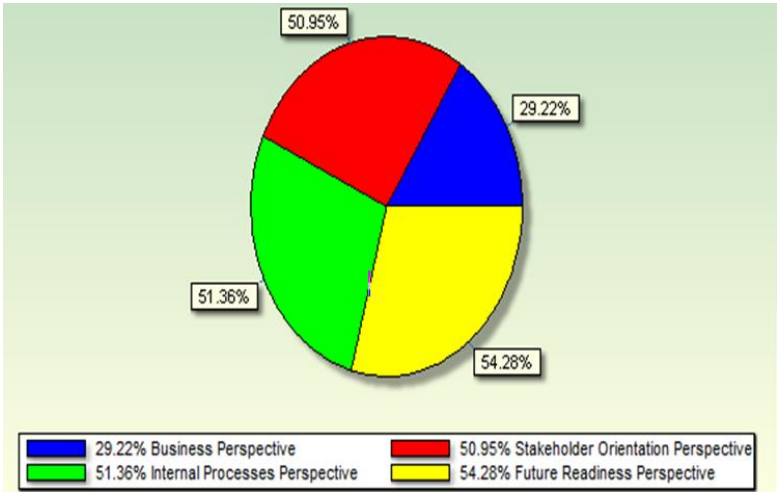

Figure 4. Example – Dashboard of H-ITsec-BSC

Therefore, the holistic performance measure is expressed as shown in formula (3).

$$Holistic_{performance}(G_k) = aggregate(Sub\_goal_{performance}(ENT_j, subogals(G_k)) \quad (3)$$

where:
G_k is any goal , $\forall G_k \in G$
ENT_j is any entity $\in ENT$, and is performing any sub goal of G_k

5. Evaluation and Discussion

Once the security projects are kicked off, several metrics are got updated including project metrics, such as time and quality, or the performance metric of the whole implementation process. The proposed performance framework has not yet been implemented practically. Therefore, we use sample data to validate the model which was validated with selected group of cyber security managers.

Figure 3 illustrates a possible dashboard for the H-ITsec-BSC for a specific goal. Assume that we have two goals $Goal_1$ and $Goal_2$ with the same weight for each sub goal. $Goal_1$ has sub goals (G_1Sg_1, G_1Sg_2, G_1Sg_3) and $Goal_2$ has sub goals (G_2Sg_1, G_2Sg_2) with the performance values (90, 95, 25) and (70, 40) respectively. The holistic performance for ($Goal_1$, $Goal_2$) are (70, 55) respectively. Although (G_1Sg_1, G_1Sg_2) are achieving better than G_2Sg_3, the holistic performance is degraded to 70 because of G_1Sg_3 associated with Entity (Ent_2). In this case, managers can take correction actions if needed.

Figure 4 shows that the (Business Perspective, Internal Process Perspective, Stakeholders Orientation Perspective, Future Readiness) perspectives are achieving approximately (29%,51%,50%,54%) respectively. Using these figures management may need to look deeply in reasons behind the low performance of business perspective compared to the other three perspectives. Note that the BSC balances between these perspectives and the numbers will not sum to 100%, but each perspective will. Also, each indicator should reach 100%, at the end of each year, once related goals are completed.

Figure 5 shows the strategy map of one CSS at a particular point of time. Managers can know the percentage of achievement at the goal level and at the strategy level. The proposed performance measure will be a very important tool in terms it will link goals and there leading and lagging indicators with the CSS. Ultimately, it allows instant view of the CSS implementation detailed status any time. Consequently, appropriate actions could be taken when needed.

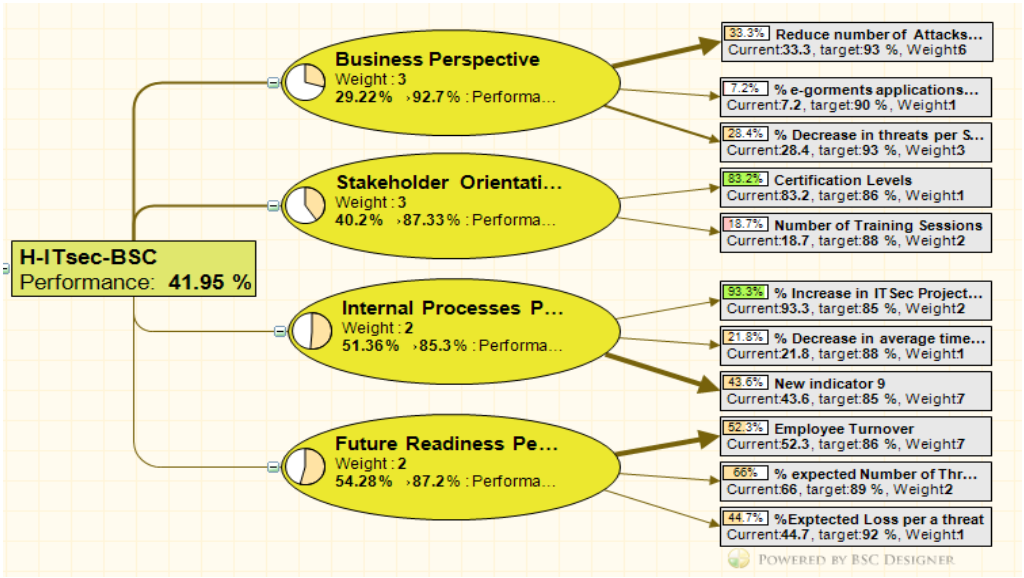

Figure 5. Example – Strategy Map of H-ITsec-BSC

6. Conclusion

In this article, we illustrated how performance of the cyber security implementation frameworks could be established by utilizing a modified version of the Information Security Balanced Scorecard, called the Holistic ITsec-BSC (H-ITsec-BSC). The H-ITsec-BSC allows performance measurement at the national level. It aggregates performance measures values from various entities executing the cyber security strategy sub goals. The aggregation is alleviated by proposing an approach that links and maps holistic goals with entities' sub goals. Therefore, the proposed H-ITsec-BSC allows the governance body of the cyber security implementation frameworks to track who is responsible for a variation between expected and current performance indicators. The H-ITsec-BSC manages, monitors, and controls the performance holistically, leaving each provider with its choice of the BSC version or any performance measurement technique as long as its metrics are exposed to the H-ITsec-BSC. The H-ITsec-BSC was applied partially on Jordan CSS as a proof of concept.

Disclaimer

This paper does not represent the thoughts, intentions, plans or strategies of the NITC, Jordan's MoICT, or any other Governmental or nongovernmental entity; it is solely the opinion of the authors. The NITC, MoICT, and/or any other entities are not responsible for the accuracy of any of the information supplied herein.

References

[1] P. Taticchi, F. Tonelli, and L. Cagnazzo, "Performance measurement and management: a literature review and a research agenda," Meas. Bus. Excell., vol. 14, no. 1, **(2010)**, pp. 4–18.
[2] S. S. S. Nudurupati, U. S. S. Bititci, V. Kumar, and F. T. S. T. S. Chan, "State of the art literature review on performance measurement," Comput. Ind. Eng., vol. 60, no. 2, pp. 279–290, Mar. **2011.**
[3] L. L. Constantine, "From virtual digits to real destruction: lessons from Stuxnet," Cut. IT J., vol. 24, no. 5, p. 6, 2011.
[4] Government of Australia, "Cyber SeCurity Strategy," 2009. [Online]. Available: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG Cyber Security Strategy - for website.pdf.
[5] Federal Ministry of the Interior, "Cyber Security Strategy for Germany," 2011.
[6] I. Atoum, A. A. Otoom, and A. Abu Ali, "A Holistic Cyber Security Implementation Framework," Int. J. Inf. Secur., vol. 22, no. 3, pp. 251–264, 2012.
[7] A. Otoom and I. Atoum, "An Implementation Framework (IF) for the National Information Assurance and Cyber Security Strategy (NIACSS) of Jordan," Int. Arab J. Inf. Technol., vol. 10, no. 4, 2013.
[8] R. S. Kaplan and D. P. Norton, "Using the balanced scorecard as a strategic management system," Harv. Bus. Rev., vol. 74, no. 1, pp. 75–85, 1996.
[9] R. S. Kaplan and D. P. Norton, "Strategic learning & the balanced scorecard," Strateg. Leadersh., vol. 24, no. 5, pp. 18–24, 1996.
[10] R. S. Kaplan and D. P. Norton, "Measuring the strategic readiness of intangible assets," Harv. Bus. Rev., vol. 82, no. 2, pp. 52–63, 2004.
[11] R. S. Kaplan, D. P. Norton, and others, "The balanced scorecard--measures that drive performance," Harv. Bus. Rev., vol. 70, no. 1, pp. 71–79, 1992.
[12] N. Klein, R. S. Kaplan, N. Chemical Bank (New York, and C. B. Corporation, Chemical Bank: Implementing the Balanced Scorecard. Harvard Business School, 1999.
[13] D. Rigby and B. Bilodeau, "Management Tools & Trends 2011," 2011.
[14] H. Norreklit, "The balance on the balanced scorecard a critical analysis of some of its assumptions," Manag. Account. Res., vol. 11, no. 1, pp. 65–88, 2000.
[15] A. György, "Finding the Right Balanced Scorecard for Business-Driven IT Management A Literature Review," Rev. Lit. Arts Am., 2012.
[16] T. Herath, H. Herath, and W. G. Bremser, "Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management," Inf. Syst. Manag., vol. 27, no. 1, pp. 72–81, Jan. 2010.
[17] A. Neely, "The performance measurement revolution: why now and what next?," Int. J. Oper. Prod. Manag., vol. 19, no. 2, pp. 205–228, 1999.
[18] P. Taticchi, "Business performance measurement and management: implementation of principles in SMEs and enterprise networks," PhD Thesis, University of Perugia, Italy, 2008.

[19] I.-L. Wu and Y.-Z. Kuo, "A Balanced Scorecard Approach in Assessing IT Value in Healthcare Sector: An Empirical Examination.," J. Med. Syst., Mar. 2012.
[20] C. Heavey and E. Murphy, "Integrating the Balanced Scorecard with Six Sigma," TQM J., vol. 24, no. 2, pp. 108–122, 2012.
[21] J. E. Goldman and S. Ahuja, "Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework," ICT Ethics Secur. 21st Century New Dev. Appl., p. 277, 2011.
[22] A. F. Marcos and J. I. Rouyet, "An IT Balance Scorecard Design under Service Management Philosophy," 2012 45th Hawaii, 2012.
[23] R. Othman, "Enhancing the effectiveness of the balanced scorecard with scenario planning," Int. J. Product. Perform. Manag., vol. 57, no. 3, pp. 259–266, 2008.
[24] J. Self, "Metrics and management: applying the results of the balanced scorecard," Perform. Meas. Metrics, vol. 5, no. 3, pp. 101–105, 2004.

