Towards Value-based Information Security Management Monitoring

Alberto S. Lima, J. Neuman de Souza
Federal University of Ceará (UFC)
Fortaleza, Brazil
{albertosampaio, neuman}@ufc.br

E. C. Branco Jr., Maristella Ribas
Federal University of Ceará (UFC)
Fortaleza, Brazil
ecastelob@gmail.com, marisribas@gmail.com

Abstract
The main objective of Information Security Management (ISM) is to align IT security with business security in all service and service management activities within an integrated strategy with corporate IT governance. To obtain a full IT-business alignment is still a challenge to managers. In continual service improvement (CSI) related activities, such as ISM, this problem is even more apparent. The actual impact upon business, due to lower quality results in ISM, is not apparent to top level executives. This article discusses an integration of ISM with a CSI approach and illustrates its benefits and gains. We proposed a value-based framework to evaluate the ISM process in a quantitative manner, whereby estimating the ISM value and quality indicators which can be used to input ISM and IT services performance in strategic planning tools. We discuss and illustrate the cause effect relation and innovations of this idea to common ISM practices.

Keywords—*Information security management; Business value and quality of IT services; Fuzzy models; Continual service improvement.*

I. INTRODUCTION

Information Security Management (ISM) is within the overall corporative IT governance strategy. It provides a strategic direction for security activities and ensures achievement of objectives, consistent information security risk management and effective information resources usage. Other pressures to ensure good governance today indicate that information security is a business-wide issue. Top level executives need to evaluate how ISM is delivering value to business, in a quantitative way. As cited in ITIL [1], the security objective is met when we have available and usable information, attack resistant systems, failure prevention and recovery. In addition, the necessity of complete and accurate confidential information, protected against unauthorized activities. Authenticity and non-repudiation guarantee that exchange of information can be trusted.

This paper discusses ISM in a *Business-driven IT management* (BDIM) [2] perspective. We are interested in ISM as one of the IT management processes cited in ITIL, which relates to ITSM improvement activities. We present a business-driven ISM improvement framework based upon the extension of our previous work [5], which is aimed at bridging the gap that still exists between BDIM concepts and actual ISM approaches in relation to business value delivery. This includes the need of using adequate metrics for presentation to top level executives, using drill-down in IT services and ISM result analysis (to obtain cause-effect relations), when considering security aspects in IT service evaluations, amongst others.

We proposed a framework to help managers in continual service improvement (CSI) related activities, with the following outputs:

- IT service and ISM estimative quality;
- IT service and ISM reference business value;
- IT service and ISM delivered business value. The delivered business value will be lower than the reference business value when quality drops.

Our main work contribution resides in the framework proposal. We treat information security management aspects related to each IT service, when estimating the IT service delivered value, ISM process delivered value and estimative quality indicators. We are still able to evaluate a more specific security service using our framework.

II. RELATED WORK

This section relates the research reported in this paper to other published work. We organized the discussion by concept, going from general to more specific concepts. At a high conceptual level, our work deals with IT Service Management with a business outlook, whereby it derives ideas from several other researchers working in a field called BDIM [2, 3]. When proposing a business-driven solution to treat incident management, a CSI-related activity, Bartolini and Stefanelli [3] observe that BDIM is the application of a set of models, practices, techniques and tools, in order to map and to quantitatively evaluate interdependencies between business performance and IT solutions. This allows the use of quantified evaluation to improve the IT solution´s quality of service and related business results. BDIM theory and practice are discussed from a decision-making perspective in [4]. The work presents the most challenging decision-making problems that researchers and practitioners have had to deal with in order to recommend future research directions.

IT services business value is another related concept. In our previous work [5], we identified a need to include security aspects related to each evaluated IT service in our business estimative value process and to estimate the value of a security service. Figure 1 shows aspects that increase the IT services delivered value to business in continual service improvement related activities. Harmon, Raffo and Faulk [6] show an example of a value-based pricing approach for a software pricing process based upon a customer perceived value in relation to received benefits. Value covers a well-defined lifecycle, starting at its creation, passing through a set of transformations and transfers, until it finally disappears [7].

978-3-901882-50-0 ©2013 IFIP

Oliveira *et al.* [7] shows that a series of entities interact and somehow contribute to create conditions and events necessary to lifecycle fulfillment. Aib and Boutaba [9] illustrate a systematic approach to business and policy driven refinement, whereby they discuss business-driven optimization and an implementation of an application-hosting service level agreement (SLA) user case.

A continual service improvement approach was proposed in Kajbaf *et al.* [10] with the presentation of an IT service reporting framework, in order to help organizations in implementing IT service improvement processes in accordance with ISO/IEC 20000 *Plan-Do-Check-Act* (PDCA) cycle and reporting requirements. An ITIL-based IT service management measurement system (ITSM-MS) and its implementation project were presented in Lahtela *et al.* [11], in order to measure the performance of IT service support processes. A cost-based framework was presented in [12] to evaluate cloud computing as a viable delivery mechanism against in-house enterprise data centers. In [13], the proposal was a framework that can allow customers to evaluate Cloud offerings and rank them based on their ability to meet the user's Quality of Service (QoS) requirements.

III. Information Security Management Improvement

We should have a close alignment of information security with business security and business needs. ITIL [1] cites that all processes within an IT organization must include security considerations.

The main reference for ISM in ITIL [1] is the *Service Design* publication, however, ISM is regularly used in context throughout the *Service Lifecycle* [14]. ISM is a component of the continual service improvement (CSI) value delivery chain (see Figure 1), whereby we have some peculiarities that managers should observe to establish an effective and integrated ISM approach in relation to business needs. As shown in Figure 1, the CSI value delivery chain includes the values generated by quality management, impact management, risk and cost management, and information security management. Our problem was how to estimate service delivered value, including quality and security aspects.

When improving the information security management aspects related to IT services, we are increasing their total delivered business value. The principal requirement in ISM is to guarantee that current and future aspects and risks be cost-effectively managed.

To manage information security, we need first to devise and recommend security measures according to organization requirements (gathered from business, service risk, plans and strategies, SLAs, OLAs and other information security responsibilities). We should still consider factors such as available funding, organization culture and attitudes towards security [14].

Special information security management aspects

When evaluating information security management at a strategic level (eg Balanced Scored Card), we need to know some topics related to information security management, such as: the actual status of an organization in relation to information security; which processes need to be improved in accordance with an organization's strategies; what are the priorities in relation to information security investments; which results will occur when prioritizing and executing improvement actions; benchmarking results to compare organizations in the same market segment; the conformity level in relation to standards such as: ISO 27001, ISO 27002 and ISO 20000 (IT service management).

ISO/IEC 27004 [15] cites that an *Information Security Measurement Programme* should include measures and measurement development; measurement operation; reporting of data analysis and measurement results, and i*nformation security measurement programme* evaluation and improvement.

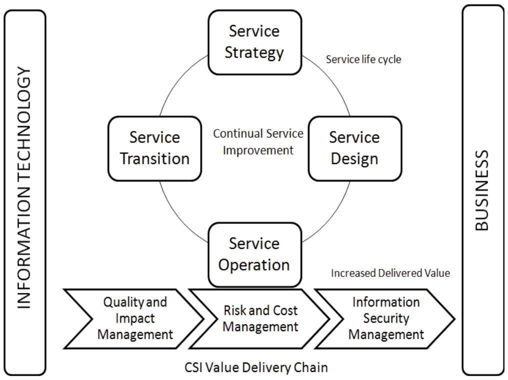

Figure 1. Value delivery chain for business-driven CSI solutions

IV. An ISM improvement framework

Measurements of the qualitative and quantitative properties of IT services have been difficult to achieve. Qualitative properties may be intangible and therefore cannot be captured via direct measurement [16]. The scale and measurement method affects the choice of analytical techniques used to produce performance indicators [15].

We consider ISM as a business process which delivers value to business (see Figure 1), whereby it has to be periodically evaluated. The ISM processes related to IT Services design should be evaluated within the IT service. We should establish ISM metrics (*key performance indicators - KPIs*), guided by ISM objectives, in order to evaluate security management of a specific IT service, whereby evaluating ISM in a general way. ISM evaluation metrics can be designed as KPIs and grouped in KQIs (*key quality indicators*), depending upon service management maturity and instrumentation tools which exist in organizations.

Managers should observe the best way to evaluate the most important aspects which can influence ISM general estimative quality using our hierarchical design monitoring approach *ISM/Service-Objectives-KQIs-KPIs*. If we consider KQIs and KPIs identification to this monitoring design, ISM documentation can be a useful bibliography to get all the necessary data to elicitations. If we want to evaluate just the IT service process related activities (Eg. ISM of IT service A), we can use the monitoring hierarchy *Process-Objectives-KQIs-KPIs*. For example, when using framework results to input a decision-making tool, we should estimate weights to

KPIs, KQIs and set objectives (see Figure 2), whereby each subset weights sum should be equal to 1.

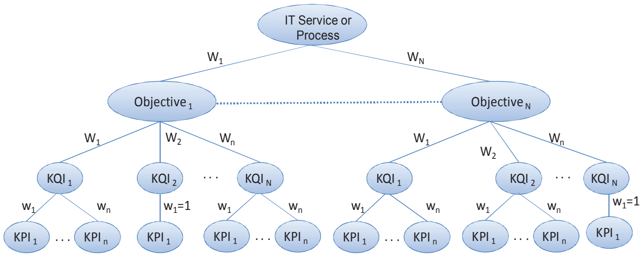

Figure 2. Framework hierarchical monitoring design for an IT service or process to input decision-making tools

The ISM process is related to various ITSM and business activities. We developed a new application view which is shown in Figure 3. Figure 4 shows the framework inputs, KPIs collected at operational level, followed by an estimative value method and an estimative quality method, which results in a quantitative output for evaluated object value and general quality percentage at hierarchical monitoring levels. We use our fuzzy logic based metrics aggregation method [5] to obtain objectives and KQIs quality results of evaluated objects.

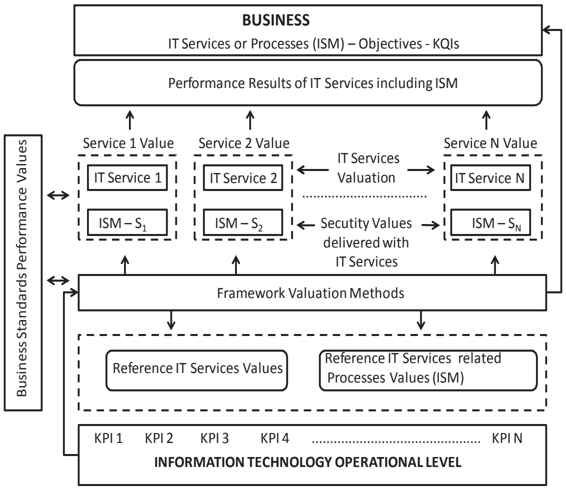
BUSINESS
IT Services or Processes (ISM) – Objectives - KQIs
Performance Results of IT Services including ISM
Service 1 Value
Service 2 Value
Service N Value
IT Service 1
IT Service 2
IT Service N
IT Services Valuation
ISM – S_1
ISM – S_2
ISM – S_N
Secutity Values delivered with IT Services
Business Standards Performance Values
Framework Valuation Methods
Reference IT Services Values
Reference IT Services related Processes Values (ISM)
KPI 1 KPI 2 KPI 3 KPI 4 .... KPI N
INFORMATION TECHNOLOGY OPERATIONAL LEVEL

Figure 3. Our ISM Framework view

Figure 3 shows our proposed business-driven ISM framework which permits ISM valuation in addition to IT services valuations. At the IT service level (see Figure 1), we should control and evaluate main service related management aspects (risk, cost, quality, impact and security). As risk and cost were not the focus of the main work, we are therefore concentrating upon security, however, risks and costs topics will be covered in future works. These methods should treat evaluated IT services within an integrated approach, which permits an effective data collection to subsidize subsequent methods in the framework.

As shown in Figure 3, security is not a step in the IT services lifecycle and cannot be solved through technology. However, it is an integral part of all IT services, whereby we have to continually manage security using controls to support and enforce security policy during service design activities.

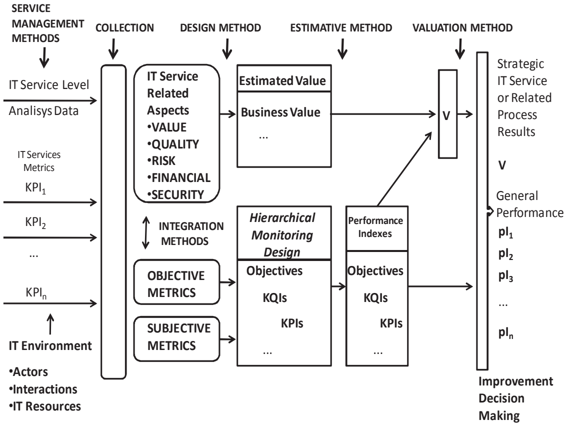

Figure 4. Framework Inputs, Outputs and Methods

Managers should have information to subsidize decisions about improvement needs, beginning at the specific point that could have generated low quality metrics. After the evaluation of IT services and related security management, we obtain the quality results when using our framework results to input a Balanced Scored Card (BSC) or decision making tool.

Valuating IT Services and ISM

The technical problem

The business problem that we must attempt to solve was described in the introduction. Let us now see how to map this to a technical problem, amenable to practical solution. Our solution will accept the following inputs:

- A set of IT services and related ISM;
- A set of service and security experts who will estimate each service/related ISM reference business value; A set of service actors who will estimate each service/ISM quality;
- The IT services and ISM related business value estimates provided by the expert evaluators;
- The IT services and ISM quality estimates provided by the service actors who are selected as service evaluators.

The framework described below is *one* solution to this technical problem and will describe particular representations for business value and quality.

Here are the desired outputs:

- The IT service/ISM groupings; evaluators may group services differently;
- The quality of each service/ISM and service/ISM group;
- The business value for each service/ISM and service/ISM group. We would like to know both the *reference* business value and the *delivered* business value.

We are evaluating IT services and related ISM when we have security components as a part of each service. If we want to evaluate a more centralized security service, we just need to estimate this security service reference business value and quality indicators.

Other than providing the above outputs, the solution should also exhibit the following important characteristics:

- Subjectivity in evaluating business value and quality must be allowed;
- Objectivity must be also allowed, wherever possible and desirable;
- Any mix of objective and subjective values must be possible;
- Epistemic uncertainty must be part of the framework. Service quality must be evaluated as part of a hierarchy of metrics. Low-level metrics are closer to tangible and measured service attributes; these metrics can then be aggregated up the hierarchy until a quality estimate for a whole service or service group can be found. The aggregation of business value should also be possible, but is only required from the service level/ISM and higher up in the hierarchy.

Our framework use is summarized as a 5 step sequence:

1. Find IT service groups and the reference business value of each group and related ISM to these groups;
2. The quality of each IT service and related ISM is expressed through low-level metrics (*key performance indicators - KPIs*). These metrics are leaves in the metrics hierarchy (Figure 2). This step expresses service quality by calculating a fuzzy number for each of these leaf service metrics;
3. The fuzzy numbers expressing quality are aggregated, starting at the leaf metrics and going up the metrics hierarchy until the (fuzzy) quality is known for all metrics (*KPIs, key quality indicators - KQIs, objectives and evaluated object*);
4. A quality index is found for each IT service group and related ISM by defuzzifying the quality (fuzzy numbers) found in the previous step;
5. The IT service and ISM delivered business value is calculated using the reference business value (step 1) and the quality index (step 4).

More details about our framework fuzzy aggregation calculus to obtain the final indexes are shown in [5]. When evaluating just the ISM process, we just follow the hierarchy *ISM-Objectives-KQIs-KPIs*. We present below a description of our calculus extensions in relation to previous methods, when integrating ISM into the IT services evaluation process.

Let

-Vg={vg_1, vg_2, vg_3, …, $\mathrm{vg}_{|G|}$}, be the IT services group set (including unitary groups), obtained in first step of our valuation method [5].

-Vsg={vsg_1, vsg_2, vsg_3, …, $\mathrm{vsg}_{|G|}$}, be the IT services security value group set (including unitary groups), obtained using the first step of our valuation method [5].

We want:

For each IT services group $\mathrm{g}_\mathrm{i} \in$ R:

$\mathrm{g}_\mathrm{i} = \{\mathrm{r}_\mathrm{W},...,\mathrm{r}_\mathrm{Z}\}$ as each IT services group $\mathrm{g}_\mathrm{i} \in$ R

$\mathrm{sg}_\mathrm{i} = \{\mathrm{sr}_\mathrm{W},...,\mathrm{sr}_\mathrm{Z}\}$ as each IT services related ISM group $\mathrm{sg}_\mathrm{i} \in$ R

and $\mathrm{W}_\mathrm{i} = \{\mathrm{w}_\mathrm{W},...,\mathrm{w}_\mathrm{Z}\}$ are the weight set of each process r_i in groups, obtained in first value estimative method step, and $\sum_{i=w}^{z} w_i = 1$. We must calculate the IT processes group (IT service and related ISM) quality percentage using individual quality percentages obtained for each individual process (IT service and related ISM) q_n and qs_n using our quality evaluation method execution [5]. Therefore, we want to obtain *qg_i (IT services)* and *qsg_i (ISM related to IT services)* :

qg ={qg_1, qg_2, qg_3, …, $\mathrm{qg}_{|G|}$} , where

$$qg_i = \frac{\sum_{i=w}^{z}(q_i * w_i)}{|\,g_i\,|}$$ **and**

qsg ={qsg_1, qsg_2, qsg_3, …, $\mathrm{qsg}_{|G|}$} , where

$$Qsg_i = \frac{\sum_{i=w}^{z}(qs_i * w_i)}{|\,g_i\,|}$$

The IT services (or group) *delivered value* is:

DVg ={dvg_1, dvg_2, dvg_3, …, $\mathrm{dvg}_{|G|}$} , where

$$dvg_i = \mathrm{vg_i} \times \mathrm{qg_i} + vsg_i \times qsg_i$$

V. An Illustrative example

We idealized four hypothetical IT services (1, 2, 3 and 4). The KPIs were fuzzified according to fuzzy logic linguistic terms, such as *no relevance*, *low relevance*, *relevant, very relevant* and *indispensable*. Figure 2 shows an example of our framework hierarchical metrics design for an IT service or process (Eg. ISM). We will use some adapted objectives cited in ITIL [1] at a business perspective, in order to give a short example of an ISM monitoring design as shown in Table 1.

Table 1. Some possible objectives for ISM monitoring

1	To protect business against security violations
2	To determine a policy integrated with business needs
3	To use justified, supported and appropriate security procedures
4	To have a mechanism for improvement
5	To be an integral part of all IT services and ITSM processes
6	To promote effective marketing and education in security requirements, IT staff awareness of the technology to support services
7	To promote operational IT security

In Table 1, the following KQIs and KPIs could be used to estimate objective 1 quality performance:

- Objective 1: To protect business against security violations
    - KQI: Security authorization promotion;
        - KPI: Security authorization promotion perception;
    - KQI: Manage account and identity;
        - KPI: Account management perception;
        - KPI: Identity management perception;
    - KQI: Decrease in breaches and incidents;
        - KPI: Percentage decrease in security breaches reported to the service desk;
        - KPI: Percentage decrease in the impact of security breaches and incidents;
    - KQI: Service Level Management
        - KPI: Percentage increase in SLA conformance to security clauses;
        - KPI: Contracts management perception;

The KPIs choice and grouping is carried out by managers that are able to use IS0 27004, the set of security controls provided by ISO/IEC 27001 or any other strategy of their choice. To input our framework, we just need to design KPIs grouped in KQIs, KQIs grouped in objectives, and so on.

The IT services quality standard reference was estimated using the framework's results of a hypothetical heuristic evaluation with 10 business specialists, including evaluators from IT and business areas. The reference business value of each IT service and related ISM were estimated by 10 managers.

We perform periodic evaluations within the metrics collected by tools and the results of a survey with the IT service's actors, used as framework inputs (ex. each month). Figure 5 shows some sequential actions to use within our framework, including aspects of ISM to calculate the IT Services and ISM process delivered value.

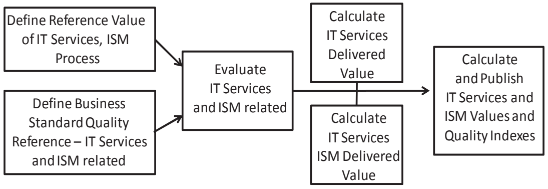
Define Reference Value of IT Services, ISM Process
Define Business Standard Quality Reference – IT Services and ISM related
Evaluate IT Services and ISM related
Calculate IT Services Delivered Value
Calculate IT Services ISM Delivered Value
Calculate and Publish IT Services and ISM Values and Quality Indexes

Figure 5. Framework use

Our framework can be used to evaluate IT services and to evaluate IT services related ISM. In this paper, our focus is to explain the calculus of information security management related to each IT service and how IT service delivered business value is increased with ISM measurement.

We show below, a sequence of steps and numerical examples of our framework use.

Step 1: Estimation of the business value of ISM related to an IT Service

The expert evaluators who are knowledgeable about a service must provide their estimate of the business value provided by the ISM related to this service. The evaluators must have previously agreed on a scale to be used so that the numerical values can be summed and compared. An evaluator may find that ISM business value should be assigned to a group of services since these services do not individually add value to the business. In this case, the business value (IT service and ISM related) applies to the whole group, but the evaluator must specify a weight for each component service. This weight aims to capture the importance of each (unitary) service within the group. As an example, suppose there are 3 services s_1, s_2 and $s_{3,}$ and that an evaluator provided the following information:

For ISM of service s_1: $(\{s_1\}, 1, 5)$
For ISM of service s_2: $(\{s_2, s_3\}, 0.4, 11)$
For ISM of service s_3: $(\{s_2, s_3\}, 0.6, 11)$

These tuples mean that the evaluator used two groups $\{s_1\}$ and $\{s_2,s_3\}$, with business values of 5 and 11, respectively. Service s_2 has a weight of 0.4 within its group and service s_3 has a weight of 0.6.

We have now obtained tuples indicating the business value for service groups from all evaluators. How are they combined? Firstly, note that evaluators may group services differently. A group specified by a particular evaluator is rejected if the component services are assigned a higher total business value by evaluators that left these services ungrouped. Rejecting a group means breaking it into unitary services and distributing the business value using the service weights. For example, if the group $\{s_2,s_3\}$ seen above were rejected, the tuples would be converted to:

$(\{s_1\}, 1, 5)$ - $(\{s_2\}, 1, 4.4)$ - $(\{s_3\}, 1, 6.6)$

After processing groups, the total ISM business value for a group can be calculated as the sum of the evaluator´s business value estimates. We use this same process to estimate *IT service reference business value* and its *ISM related reference business value* or just *ISM reference business value*.

Numerical example. Consider 4 services and 3 evaluators providing the information as shown in Table 2. Evaluator 1 suggests a group $\{s_2,s_3\}$ with a business value of 21. This group is accepted since services s_2 and s_3 have a total ISM business value of only 5+3+3+1=12, when evaluated as unitary services by other evaluators. On the other hand, the group suggested by evaluator 3 is rejected since 3+5+8+4.2=20.2 > 5. Services s_3 and s_4 are better valued singly rather than as a group. The final service grouping is $\{\{s_1\}, \{s_2, s_3\}, \{s_4\}\}$ with ISM business values of 29, 33 and 17, respectively.

Table 2. ISM business value of IT Services

IT Service ISM	**Evaluator**		
	e_1	***e_2***	***e_3***
s_1	3	13	13
s_2	21, $w_{2,1} = 0.8$	5	3
s_3	21, $w_{3,1} = 0.2$	3	5, $w_{3,3} = 0.2$
s_4	5	8	5, $w_{4,3} = 0.8$

Step 2: Estimation of the quality of IT services security management

We now turn to ISM quality. Quality is modeled by a set of metrics organized as a hierarchy (eg. Figure 2). The leaf metrics gauge the security quality of a service along several dimensions. These lowest-level metrics are called *Key Performance Indicators* (KPIs). They are aggregated into higher metrics called *Key Quality Indicators* (KQIs) that are further aggregated into service objectives, and so on up the metrics hierarchy. The estimation of service quality starts at the lowest level (KPIs) and works its way up to the top of the hierarchy. This step shows how to obtain quality estimates for leaf metrics only. The next step will show how to aggregate up the hierarchy.

For each KPI, each evaluator must supply a triangular fuzzy number to express quality along the dimension represented by that KPI. These fuzzy numbers may be constructed manually by an evaluator, or alternatively, linguistic terms may be used. For example, "good" would be represented by the number (2,3,4). The next problem is to join fuzzy numbers from different evaluators. We give more weight to evaluators whose numbers agree more and we also assign individual weights to evaluators to represent each evaluator's importance (more knowledgeable specialists for a given service are given greater weight.)

Let us first consider how fuzzy numbers agree with one another, the so called *concordance* between fuzzy numbers. The concordance between the two numbers can be calculated as the ratio of the area of intersection to the total area under the numbers. This ratio is a (real) number between 0 and 1.

Given the concordance between any 2 evaluators, we can find the mean for each evaluator's concordance with other evaluators (not including itself) and then normalize between all evaluators so that the sum is 1. This will give us the *Evaluator Relative Concordance Degree* (ERCD) for each evaluator, a (real) number between 0 and 1.

Next multiply each ERCD by the evaluator's importance and normalize again over all evaluators - this is the *Evaluator Consensus Coefficient* (ECC). The importance of each evaluator can be set as desired. One possibility which was carried out in the case study, is to apply a *Specialist Identification Questionnaire* and normalize the scores obtained by the evaluators.

Finally, the fuzzy numbers representing quality from each evaluator are summed by first multiplying a fuzzy number by its evaluator's ECC.

Numerical example. Consider a single KPI evaluated by 3 evaluators. The quality values informed by the evaluators are:

(2, 3, 4) (good) - (2, 3, 4) (good) - (3, 4, 4) (excellent)

The concordance between the first two fuzzy numbers is obviously 1. The concordance between the first and last is 0.2 (area of intersection divided by total area). From this we get ECD = [0.72, 0.72, 0.20]. A further calculation yields ERCD = [0.44, 0.44, 0.12]. Now let us assume that we have the following evaluator importance vector, gathered by applying a specialist identification questionnaire: [0.50, 0.30, 0.20]. We can now calculate the evaluator's consensus coefficients: ECC = [0.58, 0.35, 0.06]. We now use this last vector as a weight to combine the evaluator's quality values: Q = 0.58 · (2, 3, 4) + 0.35 · (2, 3, 4) + 0.06 · (3, 4, 4) = (2.1, 3.1, 4.0). This is the final (fuzzy) quality value for this KPI, after combining results from 3 evaluators.

Low-level operational metrics are often automatically gathered by monitoring tools. How can these objectively-measured KPIs be introduced into the above calculation? One can use a mapping function, such as the one shown in Figure 6 to fuzzify the measures. This mapping function will typically be set up from parameters present in the *Service Level Agreements (SLAs)* to which the service is subjected to.

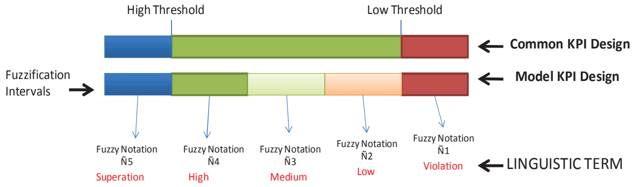

Figure 6. Fuzzification rule for quantitative KPIs collected in IT environment

Step 3: Metrics aggregation

We now have a fuzzy estimate for leaf KPIs and we need to aggregate these to find a fuzzy estimate for metrics higher up in the hierarchy. This is carried out at all points in a manner analogous to the last step, whereas the last step aggregated fuzzy numbers from several evaluators. We now wish to aggregate fuzzy numbers from several children to find the parent value. Here are the steps:

1. Find the concordance between child fuzzy numbers. The case of there being no concordance is treated in a special way not discussed here. Basically, it uses negative numbers to represent how far apart the non-overlapping fuzzy numbers are. A full explanation is given in [5].
2. The mean concordance is found for each child and normalized yielding of the *Metric Relative Concordance Degree* (MRCD).
3. Multiply each MRCD by the child metric's importance and normalization, yielding the weight of the child metric. The child importance is taken to be the fuzzy number's mean value.
4. Sum all child metrics by first multiplying each fuzzy number by the corresponding child's weight.

Numerical example. Let us aggregate the following 3 metrics, children of a common parent: (2.0, 3.0, 4.0), (2.0, 3.0, 4.0), (3.0, 4.0, 4.0). The concordance vector is [0.82, 0.82, 0.60] which is normalized to yield the MRCD: [0.37, 0.37, 0.27]. The metric importance vector is found by normalizing the mean fuzzy values. The values are 3.0, 3.0 and 4.0, or after normalization: [0.30, 0.30, 0.40]. Combining MRCD and the importance vector yields the following metric weight vector: [0.34, 0.34, 0.33]. The final aggregation proceeds, thus resulting in the fuzzy number: (2.3, 3.3, 4.0).

Step 4: Calculation of ISM quality

Our goal in this step is to defuzzify the quality metrics. For that purpose, we ask: "How much of this fuzzy number's pertinence function falls in an area considered of acceptable quality?" This implies that we have information concerning what is acceptable quality. The service experts are asked to specify a (fuzzy) *Reference Quality Standard.* This is similar to what was carried out in step 1, except that we now want them to define the *desired* quality rather than *actual* quality of a service. We now want to compare two fuzzy numbers: the one representing actual service quality and the other representing the desired standard.

We cannot simply calculate the overlap, the reason being is that actual quality may be *better* than the desired standard. Naturally, in this case, we want to count the actual quality as "good", even though it may not overlap the standard. We proceed as follows: extend the reference triangular fuzzy number to the right as far as possible and make it trapezoidal; the overlap with the trapezoidal number will now represent the degree to which actual quality attains the desired standard.

Numerical example. Let us continue the numerical example in step 3. The result was (2.3, 3.3, 4.0). Now assume that the reference quality standard obtained from the evaluators is (3.2, 3.5, 3.6). This can be expressed as the following trapezoidal fuzzy number (3.2, 3.5, 4.0, 4.0). We can calculate the quality index as 0.39 (intersection area = 0.33, total area 0.84).

Step 5: Estimation of delivered business value for ISM related to IT service

Step 1 yielded the business value that an ISM of a service (or service group) should ideally deliver, that is, with perfect ISM quality. Step 4 has given us ISM quality as a number between 0 and 1. Assuming a linear relationship between quality and actual ISM business value delivered, we can calculate an ISM delivered business value as the ISM ideal business value times the ISM quality.

Numerical example. In step 1, we calculated the business value of ISM of service s_1 to be 29. With a quality of 0.39 from step 4, the ISM delivered business value of service s_1 is 11.

The final values obtained in our example to all ISM related to each IT service are shown in Table 3.

Table 3. ISM delivered value of IT Services

ISM related to IT service	Reference Business Value	Quality percent	Delivered Value
S_1	29	0.39	11
S_2,S_3	33	0.8	26.4
S_4	17	0.94	15.98

Using our framework, we obtained the IT services business and delivered values which are show in Table 4.

Table 4. IT Services business and delivered values

IT service	Reference Business Value	Quality percent	Delivered Value
S_1	11	0.8	8.8
S_2,S_3	37	0.6	22.2
S_4	10	0.94	9.4

To obtain the IT Service delivered value that includes the ISM aspects, we should sum the delivered values of IT service and ISM related to the IT service (See Tables 3 and 4). For example, the delivered business value of IT service S_1= 8.8 + 11 = 19.8. We show in Figure 7, the IT services delivered values and related ISM delivered values.

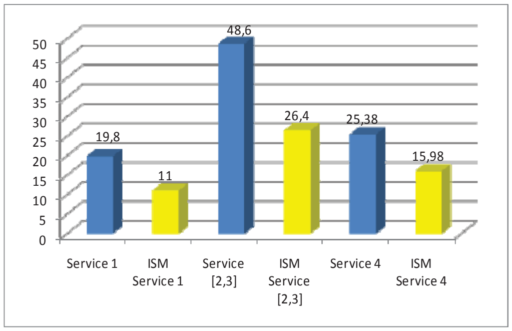

Figure 7. Illustrative example of framework business value reference

The measurement of security aspects related to each IT service is a part of the global IT service delivered value. Because of the importance of security management, we think that the ISM business value has to be examined by managers as an important component of CSI value chain.

VI. A WORK IN PROGRESS FACE VALIDITY

Framework initial face validity. Are we able to believe in the numerical outputs provided by the framework - Is the framework useful, and to what extent – Is there performance improvement in the ISM process? Answering such questions and validating a complex framework such as we have presented here, is a multi-year effort.

We have work in progress at a Brazilian IT company, whereby we executed a preliminary evaluation and used a fast-lane approach, establishing our theory face validity. In other words, does the framework appear reasonable on its face to people who are knowledgeable about the real system? We adapted our previous work [5] face validity questionnaire, which was applied to ten managers of companies in the industrial, bank (finances) and IT sectors. Some of them were already aware of our previous work. The questionnaire included nine questions, each of which leads to a hypothesis to be tested. Since the population of managers is much larger than ten, statistical inference was used to test the hypotheses. The complete framework theory was presented to the managers before the evaluation. A binomial statistical test with a 5% significance level was used to produce the results as shown in Table 5.

Table 5. Hypotheses to test theory face validity

Hypothesis	% who agree	Is there statistically significant evidence to accept hypothesis?
Preference: Manager prefers the framework to the current evaluation process	100	yes
Utility: Manager considers the framework useful	100	yes
Completeness: Manager considers framework satisfactorily complete	60	no
Accuracy and precision: Manager considers framework sufficiently accurate and precise	80	yes
Effectiveness: In modeling a business scenario, manager can identify quality and value elements	90	yes
Effectiveness: In modeling a business scenario, manager can estimate quality and value elements in numerical or linguist terms	100	yes
Reliability: Manager considers that the framework improves the quantification of value in terms of reliability	90	yes
Trustworthiness: Manager consider that the framework improves the quantification of value in terms of trustworthiness	100	yes
Intangibles: Manager consider that intangible elements of Value can be identified and quantified	100	yes

Face validity appears to be established in all dimensions analyzed, except that of *completeness*. It is especially important to note that managers considered the framework to be "useful" and "preferable" to the current way of evaluating ISM and IT services. The questionnaire does not cover all dimensions, of course. We gathered additional insights through talks with the managers. The following additional problems were identified: 1) there is a steep learning curve to understand the mathematical calculus; and 2), there is too much data to be inputted into the framework. Since framework internals need not be known by the managers who use it, we can discount the first problem. However, the second problem, subjectivity, remains at a price. Subjectivity demands more effort than the use of automatic tools to obtain data. However, pursuing this approach seems to be worthwhile since managers consider the framework preferable to their current approach. This same face validity test will be repeated after the real case study in due course.

VII. FINAL CONSIDERATIONS AND FUTURE WORK

This paper outlined a framework to improve ISM using a BDIM [2] feedback monitoring strategy. This value-based approach is linked to continual service improvement related activities.

What have we achieved? We proposed a framework, extending the calculus of our business-driven model [5] to capture ISM process delivered value and quality of IT processes in relation to a corporative standard created using our framework. Our framework can be used to evaluate ISM linked to IT service evaluations or just ISM as a process. This framework is different from our previous works, and within this framework, reside our contributions, in that: it captures the impact on the business of processes imperfections; it represents epistemic uncertainty; it treats subjectivity; and it includes ISM measurement in the valuation process.

Our framework is appropriate to be used in an ISM process, because it allows drill-down from high-level metrics (effects) to those of low-level (causes). The framework is applicable in any organization that provides IT services using ITIL processes. Our framework results can be used to input *balanced scored card* (BSC) tools (to be used by top level executives), to identify improvement requirements in security of IT services or in a more centralized security service and to rank the results in periodical comparative analysis.

What are the main conclusions? Preliminary studies indicate the usefulness of the approach in assisting IT executives in defining more easily business-driven feedback in ISM monitoring, using an improvement view.

Managers generally accept the model at initial face validity. Specifically:

- Managers prefer our approach in relation to their standard way of evaluating security management and IT services;
- Managers find the framework to be useful in performing CSI related activities;
- Managers are satisfied with the framework's accuracy;
- Managers think that identifying quality and business value elements required by the framework is feasible;
- Managers are able to estimate quality and business value, either numerically or through linguistic terms;
- Managers find the framework to be trustworthy and reliable;
- Managers believe that the framework can capture intangibles.

We can enumerate the following advantages for using our ISM improvement framework in addition to conventional ISM methods: business IT alignment at strategic and operational levels in IT process evaluations such as ISM, generating value to business; a simplified subjectivity treatment involved in metrics evaluation; non-intrusion to conventional approaches; value-based approaches in addition to conventional ISM strategies; flexibility and adaptability to various business scenarios.

What are the future works? Research efforts leading to broader validation campaigns are ongoing. We feel that future works should focus on testing our framework to evaluate ISM and IT services in a cloud computing IT services organization. We would also like to pursue the following directions: add aleatory uncertainty (aleatory uncertainty means that metric values change due to the natural stochastic nature of physical processes); make business value more concrete by monetizing it; include risk and the decision makers' risk attitude; link the model to a *balanced scorecard* and better model strategic aspects of the business to input decision-making tools; propose decision-making approaches to CSI and ISM monitoring.

REFERENCES

[1] OGC (Office of Government Commerce), ITIL V.3 PUBLICATIONS, “Service Strategy”, “Continual Service Improvement”, “Service Design” “Service Operation”, “Service Transition”, 2007.

[2] Moura, J. A. B. Sauvé J. P., Bartolini C., “Business-driven IT management–upping the ante of IT: exploring the linkage between IT and business to improve both IT and business results ”, IEEE Commun. Mag., vol. 46, no. 10, pp. 148–153, 2008.

[3] Bartolini C., Stefanelli, C., “Business-driven IT Management,”, Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 963 –969, 2011.

[4] Bartolini C., Stefanelli C, Tortonesi M., “On decision making in business-driven IT management ”, in Proc. 2011 IFIP/IEEE International Symposium on Integrated Network Management, pp. 1082–1088, 2011.

[5] Lima, A. S., De Souza, J. N., Callado, A. C., Oliveira, J. A., Sauvé, J., Moura, J. A. B., “A Business-Driven IT Services Improvement Model”, Proceedings of the Forth International Workshop on Distributed Autonomous Network Management Systems – DANMS. IEEE Communications Society, 2011.

[6] Harmon ,R., Raffo , David, Faulk ,S., “Value-Based Pricing for New Software Products: Strategy Insights for Developers”, in www.cpd.ogi.edu/MST/CapstoneSPR2005/VBSP.pdf.

[7] Oliveira, J. A., Moura, J. A. B., Bartolini, C., Hickey, M., Sauvé, J. “Value-based IT Decision Support - Towards a formal business value model for steering IT-business alignment”, 4th IEEE/IFIP International Workshop on BDIM, 2009.

[8] Oliveira, J. A., Sauvé, J., Bartolini, C., Moura, J. A. B., Hickey, M., Queiroz M., “Value-driven IT Service Portfolio Selection under Uncertainty”, 2010 IEEE / IFIP International Network Operations and Management Systems (NOMS), 2010.

[9] Aib, I. and Boutaba, R., “On Leveraging Policy-Based Management for Maximizing Business Profit” in: IEEE Transactions on Network and Service Management, 4(3), pp. 25-39, 2007.

[10] Kajbaf, M., Madani, N., Suzanger, A., Nasher, S., Kalantarian, M., “An IT Service Reporting Framework for Effective Implementation of ITIL Continual Service Improvement Process Conforming to ISO/EC 20000”, in: Proceedings of Fifth International Conference on Digital Society (ICDS), 2011.

[11] Lahtela, A., Jantti, M., Kaukola, J. A. Lahtela, M. Jantti, and J. Kaukola, “Implementing an ITIL-based IT Service Management Measurement System”, in: Proceedings Fourth International Conference on Digital Society, St. Maarten, pp. 249-254, 2010.

[12] Sripanidkulchai K., Sujichantararat S., “A Business-Driven Framework for Evaluating Cloud Computing”, Proceedings of 2012 IEEE/IFIP 7th Workshop on Business Driven IT Management, 2012.

[13] Garg S. K., Versteeg S., Buyya R., “A framework for ranking of cloud computing services”, Future Generation Computer Systems, http://dx.doi.org/10.1016/j.future.2012.06.006, 2012.

[14] Clinch J., “ITIL v.3 and Information Security”, Clinch Consulting, White Paper, 2009.

[15] ISO/IEC 27004, first edition, “Information technology-Security techniques - Information security management-Measurement”, 2009.

[16] Radack, S., “Security Metrics: Measurements to support the continued development of Information Security Technology”, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, white paper, 2010.