A Case for a Process-based Approach to GRC

A number of corporate accounting scandals, such as Enron, created a need for regulations, such as the US Sarbanes-Oxley Act. The need for sound corporate governance principles was actively debated in this context, and the concept of governance, risk management and compliance (GRC) resulted. The concept has wide coverage now, encompassing enterprise risk management (ERM), operational risk management, incident management and other related areas. As with many popular concepts and practices, there are myths surrounding GRC, too. Some of these myths include:

• GRC is for the board to worry about; day-to-day management is not concerned with GRC.
• GRC is for big companies only.
• GRC is for listed companies to worry about.
• GRC is about documentation and reporting.
• GRC implementation interferes with the business.

Irrespective of size and pattern of ownership, organizations need to recognize that governance is the superordinate requirement to sustain ongoing activities, and risk management and compliance are necessary prerequisites for ensuring good governance. Thus, GRC needs to be a critical concern for all organizations, and its focus should be much larger than statutory compliance.

A narrow focus has made GRC a reactive and piecemeal exercise in organizations. Even larger organizations with a better vision of GRC take up statutory compliance as the first step, and the larger exercise of holistic implementation and maintenance of GRC is placed at a lower priority. Consultants who are engaged in these assignments are forced to cater to the immediate needs of management and, thus, fail to present a comprehensive approach of ERM as part of GRC.

The subject of this article is to present a more fundamental approach to GRC and to suggest the most appropriate methodology to make the exercise sustainable. Such an approach puts additional responsibilities on information systems (IS) auditors as well (this is addressed toward the end of the article).

Typical GRC implementation approaches include:

• **Checklist-based**—For reasons cited previously, organizations implement GRC as a reporting exercise. Implementers and auditors adopt the checklist approach for testing compliance to a list of requirements.

• **Asset-based**—In this method, information assets and their vulnerabilities are identified. Threats that could compromise confidentiality, integrity and availability of these assets are then identified. Based on the probability of threats exploiting these vulnerabilities and the consequential impact, the risk exposure is computed. Risk mitigation measures are suggested for vulnerabilities with risk exposures higher than the risk tolerance limit. The methodology is the application of Failure Mode and Effects Analysis (FMEA), popular in engineering design and analysis, to the IT domain, except that FMEA does not recommend an asset-based approach. Though the International Organization for Standardization (ISO) does not recommend any specific method for information security assessment, consultants and practitioners have been using this method for ISO 27001 implementation. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method, developed by the Software Engineering Institute (SEI), is another asset-based method.

• **Incident-based**—Another approach that is recommended for risk management and audit is to look at the past deviations, using incident reports, error reports, system failure reports, etc. Using loss-event data collection as a measure of operations risk exposure, as recommended by Basel II, is an example of an incident-based approach.
A checklist-based approach is environment-specific and lacks rigor. However, this approach is popular for audits because of its simplicity. It is useful for regular periodic audits and serves the purpose when there has not been any major change in the business processes.

An incident-based approach assumes that if there is a problem in the system, it would be visible in some of its effects. To what extent is this true? To take an analogy of the human body, a viral infection would manifest in symptoms such as a cough and a cold, so monitoring external symptoms could unearth the underlying malady, but there could be a possibility that some dormant phenomenon such as cell mutation could go undetected until it develops into cancer. Incidents provide clues to the level of exposure and allow organizations to recalibrate their business processes to meet the new exposure levels. But, if the incident turns catastrophic, it is too late for any remedial action. The recent collapses of several financial institutions despite implementation of Basel II recommendations are examples; these collapses did not leave any time for recomputation of capital requirements.

An asset-based approach is more rigorous and comprehensive than these two approaches. In this approach, risk is looked upon as a threat to an asset, and the remedial measures are incorporated in the business processes of the organization. In the subsequent sections, an argument is presented that instead of looking at the processes for remedial action only, one needs to apply a rigorous analysis to the process(es) associated with the management of assets.

The argument is based on the premise that incidents or threats to assets are due mainly to process vulnerabilities. These vulnerabilities could arise due to poor design of processes or controls associated with these processes or due to their improper implementation. Hence, a fundamental approach to risk analysis should start with process analysis.

A fundamental approach to risk analysis should start with process analysis.

PROCESS-BASED APPROACH: EXPLAINING THE RATIONALE
Risks arise because of exploitation of a vulnerability in the process. During a given period, a vulnerability may or may not result in some form of damage to an asset. It may or may not show up as an incident. Regardless, the fact remains that the vulnerability exists, ever ready to be exploited. When a risk emerges and becomes conspicuous to the users, it may have already caused damage to the processes/assets of the organization; therefore, any attempt to address risks without studying the vulnerabilities would amount to remediating the consequences without addressing the causes. That is why it is advised that the processes need to be studied for their vulnerabilities. The reason many frauds are perpetrated by internal people is because of their knowledge of vulnerabilities in the business processes.

The suitability of a process-based approach can be appreciated through a case example: A large chemical manufacturing organization had a problem in which many vendor checks were returned because of spelling mistakes in the name of the vendor. The vendor master had 4,000 entries, and the uncontrolled entry by many assistants had led to several names being misspelled. Since spelling mistakes did not create any problem in order execution, the purchase department, owner of the table, did not take any measure to correct the table. Accounts requested a facility for correcting the names while preparing checks. This was approved by management. While trying to address recurrent vendor complaints and associated problems, management did not realize that they were introducing a control weakness. No violation was reported during the six months in which this procedure was occurring; therefore, incident-based audit failed to capture the vulnerability. Asset-based risk assessment showed the vendor check returns as a threat to company reputation, an important asset, and the name correction facility for the accounts as an alleviation measure, thus the assessment showed reduced risk. It was only when the process was analyzed that the risk introduced became apparent.

PROCESS-BASED APPROACH: AN OVERVIEW
A process view of an organization is a very detailed view and requires progressive elaboration until all elemental tasks are identified. Insiders in an organization would have only a partial/gross-level view of the processes and, thus, may not be fully aware of the vulnerabilities in the processes. A detailed documentation, mapping all business processes at their elemental level, is a necessary first step. Many vulnerabilities arise at the interprocess interface level and, thus, get omitted when processes are mapped in an isolated manner by their respective owners. The level of details required
for documentation of all the business processes makes it a daunting and cumbersome task that many organizations are hesitant to undertake. But, this is a onetime task that organizations need to complete, after which the process maps need to be maintained. The latter is a manageable task if undertaken on an ongoing basis.

A structured way of understanding an organization is to take a hierarchical view of the processes. This would help one understand the relationship of the processes to the business goals as well as the interrelationship among the processes. Hierarchy starts with deliverables in terms of products/services, and then the associated business processes for these deliveries are identified. Processes need to be decomposed into subprocesses and activities. The process map is complete only when the following have been identified:

- The roles that perform each of the tasks
- Entities, including assets, impacted by the processes
- Application programs affecting the process
- Data (tables) affected by the process
- Documents used by the process (data and documents used by this process would provide a link to the process that generated the data/documents)
- Documents generated by the process
- Controls built into the process

The controls built into the process give an idea of the risks identified, and the process analysis should include the residual risk after the controls.

**AUDIT**

The process-based approach puts additional responsibilities on GRC auditors, too. GRC auditors should take a process view and check the processes. Obviously, the auditor has to undertake a sampling test to conduct the audit. While selecting processes for audit, some or all of the following criteria may be applied:

- Criticality of the process to the business
- Financial implication of the process
- Processes involving outsider interaction
- Customer interaction processes
- Recently changed processes

Depending on the level of maturity of processes, criticality of business and frequency of audit, the auditor may decide to perform a substantive audit to check the robustness of the processes as mapped or a compliance audit to check the match among the practices and processes.

In organizations in which extensive documentation of the processes exists, the auditor needs to check the conformance of the process document to the process in practice. If there are deviations, the process map has to be changed, and then the process needs to be analyzed for its robustness. This check has to address the following queries:

- What are the process objectives?
- How are they aligned to business objectives?
- What are the sources of data for this process? Are these data authenticated?
- What are the direct data entries into this process? How are they authenticated?
- What are the checks built in the process? What are the stated objectives of these checks? Are they sufficiently robust to achieve the desired objective?
- Which are the roles that hold data entry/modification rights in the process? Do these roles have sufficient authority to perform these actions?
- What are the implications of such data change/wrong data entry?
- What are the checks available for entry of accurate, authorized data only?

This is an indicative checklist and needs to be modified depending on the process and the context.

Where process maps do not exist, the auditor has the challenging task of preparing the maps for the processes identified for audit. Audit firms may need to build in-house expertise in developing business process maps or usage of business process management (BPM) tools.

**AN EXAMPLE**

The following banking example is provided to help explain the four-step process-based approach:

1. Business processes are designed in an organization with a view toward delivering a product/service. Therefore, in a top-down approach, identify the products/services delivered by the organization (see figure 1).
2. Identify the business processes associated with each of the products/services. This example takes personal loans as the product example and maps their business processes (figure 2).
3. Take the presanction subprocess and expand it (figure 3).
This step can iterate several times until the elemental level of tasks is reached. While mapping the subprocesses/activities, also map the following:
• Roles associated with the subprocess/activity (shown in gray rectangles in figure 3)

During an audit, the auditor has to independently draw the map for risks and ensure that all risks have been identified by the process owner.

4. For each of the risks identified, map the controls (figure 4).
During the audit, the auditor should check that, for all identified risks, the controls available are adequate.

CONCLUSION
This article reviews different risk analysis approaches and argues that a process-based approach addresses the requirements from the basic details and, hence, is more rigorous and comprehensive. The GRC approach has evolved beyond Sarbanes-Oxley compliance, and the GRC tools are maturing to address comprehensive risk management needs. There are process-based GRC tools currently available in the market.12

A sound GRC model would mandate the maintenance of a business process maps repository in the organization. The challenge lies not only in creating and storing these maps, but also in maintaining them. In a dynamic market situation, organizations keep adding products and services. Market demands compel organizations to continuously improve their business processes to suit the newer products and services. Even organizations that offer a fixed portfolio of products...
and services need to innovate their business processes to maintain their agility and competitiveness. These changes need to be reflected in the business process maps, and a good configuration management of these maps is essential.

Auditors should also redefine their process-based approach and should build the necessary competencies to fulfill this task. Irrespective of the organization’s approach toward GRC implementation, auditors should undertake a process-based approach, as this addresses the risk at the most elemental level and is, thus, more comprehensive. This approach has already gained popularity among larger consulting and audit firms because of its strengths.13

**ENDNOTES**

1. There are checklists made available by popular software vendors such as SAP and Oracle. Consulting organizations develop and use checklists based on their experience.
2. A detailed discussion on this technique can be found at the FMEA Info Centre site, www.fmeainfocentre.com.
3. The implementation approach can be seen on any of the ISO 27001 consultant sites. For example, www.hsc.fr/services/acccompagnement27001.html.en is one such site that recommends an asset-based approach for risk assessment.
5. The framework document explaining the approach is available at www.sei.cmu.edu/library/abstracts/reports/99tr017.cfm.
8. Nir, Karen; Sumit Anand; Sam Mannan; “Calibrate Failure-based Risk Assessments to Take Into Account the Type of Chemical Processed in Equipment,” Journal of Loss Prevention in the Process Industries, May 2006. While this article deals with risk in chemical processes, the underlying concept of incident-based risk assessment is applicable to business processes as well.
9. This issue has been reviewed critically, though not extensively, by Harald Benink and George Kaufman in “Turmoil Reveals the Inadequacy of Basel II,” Financial Times, UK, 28 February, 2008. The authors forcefully argue for a revised approach for capital computation in view of the financial sector collapses.
10. This is one reason why a good BPM tool should be used. As of 2009, Gartner identifies 22 major vendors for BPM tools (Hill, Janelle B.; Michele Cantara; Marc Kerremans; Daryl C. Plummer; “Magic Quadrant for Business Process Management Suites,” Gartner RAS Core Research Note G00164485, 18 February 2009).
11. The author thanks V. Ganesh, an experienced banker and consultant with Thesys Technologies, Chennai, India, for providing valuable inputs for creating an example.
12. For example, BWise and ARIS are two popular process-based GRC software tools.

**EDITOR’S NOTE**

Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at www.isaca.org/knowledgecenter.