IT General and Application Controls: The Model of Internalization

Industrial and financial companies sometimes find themselves faced with the choice of outsourcing IT audit services related to IT general controls (ITGC) and IT application controls (ITAC). The decision to outsource is most likely due to financial reasons, timing and/or insufficient resources, or an uncertain (if not absent) level of competency related to the enterprise that is being audited. In particular, the technical and practical knowledge of ITGC/ITAC goes well beyond the theoretical point of compliance contained in texts such as IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition (a strict reference for most companies subject to the US Sarbanes-Oxley Act), rather than management process models such as COBIT 4.1 or the IT Infrastructure Library (ITIL). In fact, it is not just a compliance matter. The practice of implementing ITGC/ITAC provides added value in identifying and correctly understanding risks and, practically, in immediately establishing an appropriate audit strategy for the entire year.

Therefore, a certain degree of experience is mandatory, but not always available, among internal audit services. To account for this deficit, companies can choose to outsource the service (at best)—unconsciously deciding to miss an important educational goal that would be achieved over time, in favor of achieving an immediate and practical objective. That choice is not farsighted given the considerable risk taken.

In fact, the main risks are precisely that: incorrectly identifying all the risks and, more than likely, having a process limited to an operational, a financial or a compliance vision—any vision except IT, which is often the first, essential means by which all the processes are structured. It could also mean missing the opportunity to create the foundations for the futuristic “integrated audit,” a model that every mature audit department aims to utilize.

MISSED OPPORTUNITIES WHEN INTERNAL AUDIT IS OUTSOURCED

Outsourcing does not give audit services the opportunity to understand business processes in their entirety. Internal auditors cannot grasp the true meaning of all business processes if they cannot understand how the information is managed across the company. All data are information used in the company to create and manage the business. Handling and understanding the information systems framework and its availability, origin and nature give the auditor a mastery of the knowledge of the risks, which represents an omnipresent goal in achieving the view of the integrated audit business model that is being discussed.

The first and last structural unit of the corporate world is represented by the data themselves. All processes are moving through the dense cluster of IT, and those processes are effective due to the efficient governance of the data. COBIT effectively summarizes this concept in its references to the research of strategic alignment between IT and business. Although the IT department can be seen as a holding company (with its budget, customers, internal suppliers and strategic objectives)—fully independent and well structured—IT can become a winning factor positioned within the strategic business. IT strategies, projects, objects and goals are the goals of the company; they support the enterprise, at minimum, and, at best, enable the enterprise to realize its success. Thus, the entire budget for IT projects is spent to support the business. All projects should come out of the business strategy and be approved and identified by the board of directors or management at the highest levels possible. No discrepancy or quantifiable or identifiable differences should exist between core business and IT strategies. The best strategy should minimize the differences as much as possible.
It is clear that, very often, internal auditors perform a lot of testing, and especially in terms of outsourcing, the complete definition of ITGC/ITAC and the evaluation control results that rely on other audits are often forgotten. However, starting with a certain degree of awareness and an established approach to ITGC can enable auditors to immediately see what was and what will be the company’s business strategy, the structural changes, the process change that concerns the data, and the information (and, therefore, the business process) during the period. For example, just checking the number and significance of program changes performed during the period is helpful. Therefore, outsourcing these control tests can create a gap of knowledge that is not always immediately or easily remedied.

THE IT DEPARTMENT—A COMPANY WITHIN THE COMPANY
From the issuance of a client order, accounts payable (AP) and wire transfers to suppliers and payroll, all company processes move through the structure and substance of the information data.

An IT department can be defined as a company within the company. The IT department usually has its own portfolio of suppliers and customers (generally subsidiaries, branches or even single departments of the holding company itself), which, of course, rarely coincide with the suppliers and clients of the holding company as a whole. For example, the finance department can become a “customer” of the IT department when there is an assistance request or when support is needed to create a new computer program in-house. Perceiving a management information system (MIS) department as a company within a company contributes to the change from the old “data center” into a value-added business unit that is business-oriented and strategically aligned and guided by principles of effectiveness and efficiency.

In the end, the opportunity to create an IT department to support the business is surely a management task that needs to be approved through the corporate governance of the board of directors, which should always remain independent.

It is also true that the internal audit department, unlike external audit and consulting, has a full commitment to corporate knowledge, which tends to focus on a standard of achievement and not on mere compliance with relevant laws and regulations. The knowledge of business risks in their entirety, of the control environment, of the company tone and culture, and of possible operational gaps gives a relevant opportunity for assessment that possibly only internal auditors can best use in the performance of their duties. For example, when experiencing a change in the supply chain process (awareness acquired during a specific internal audit), a risk concerning particular ITGC or ITAC could easily arise. Indeed, the impact of such a change may not be obvious within the mapping of the IT process, but it can be very significant when linked to the information received. Sometimes, interviews with IT management or the head of the finance department could be insufficient to detect changes because one cannot assert a priori that the communication inside the organization is efficient and effective. Thus, it is possible for an auditor to have a full understanding of a company (as COBIT recommends) only when an enterprise has applied the specific strategic alignment between IT and business.

The internalization of ITGC/ITAC is an important path to the integration of fundamental IT governance knowledge within corporate assets.
fairly assured that the business processes that go through the corporate network have a chance to be concretely realized. If the understanding of the company does not pass through the information infrastructure, it is probable that the entire business processes and relative risks cannot be understood completely.

ITGC/ITAC provide value immediately in terms of IT governance knowledge and the maturity model of the processes that the auditor has to test. Furthermore, testing ITGC/ITAC gives the enterprise the chance to assimilate fundamental requirements on controls and related risk, creating added value and knowledge on IT governance.

It can be said that the internalization of ITGC/ITAC is an important path to the integration of fundamental IT governance knowledge within corporate assets. The development of synergies between corporate governance and IT governance creates the opportunity to discover an interesting map of risks, and obviously, these synergies are applicable only within the company. This is an incredible opportunity for the auditor to use rigorously during the audit cycle. This renewed awareness will provide companies with immediately visible benefits in the form of an annual audit plan that is strategically built on a fully integrated understanding of risk.

During an audit plan, the auditor needs to verify that internal controls are effective to assure stakeholders of the true and fair representation of the financial statement. Figure 1 depicts that, although the financial statement has its financial measurements and evaluations as financial assertions externally, within the company all data come out of the process cycles of the company. The company is a group of business units crossed by processes; summaries of processes can create process cycles. With ITGC, the auditor tests the processes related to the MIS department, which is a business unit that supports all business units and processes. For this reason, ITGC are reliable for other processes and audits. ITAC concern processes and, with US Sarbanes-Oxley Act test controls, give evaluations of the validity of the controls on process cycles. The controls are implemented by management to cover the risks identified by the company. To have a good knowledge and evaluation of all the risks, it is necessary to

---

**Figure 1—An Integrated Approach: Mix of Controls**

Financial Statement

<table>
<thead>
<tr>
<th>P=Process</th>
<th>P n= Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X ) = Sarbanes-Oxley tests</td>
<td>( X ) = ITGCs</td>
</tr>
</tbody>
</table>

**Assertion IT World (CAVR):**
1. Completeness
2. Accuracy
3. Validity
4. Restricted access

**Financial Assertions:**
1. Accuracy—A
2. Completeness—C
3. Cut-off—CO
4. Existence—E/O
5. Occurrence—E/O
6. Classification—P/D
7. Understandability—P/D
8. Rights and obligations—RO
9. Valuation and allocation—V

As indicated in ISA500.15.

**Note:**
1. Narratives are written in order to perform the testing on cycles not always immediately concerning the financial statement.
2. The risk control matrix encompasses the financial assertions to value the proper risk assessment.
3. Audit financial accounts cannot consider the IT controls.

test IT governance through ITGC/ITAC and, then, through the business processes. The most in-depth audit concerns IT controls; performing this audit correctly enables enterprises to see more easily the interconnections of business processes and the related risks. The sequence of ITGC/ITAC and other audits is qualified and improves the audit quality when a systemic and methodological approach is followed when performing audits.

CONCLUSION
Implementing in-house ITGC/ITAC is a great opportunity for auditors to improve their knowledge of the company, and for the company, it is a chance to build IT governance that strengthens corporate governance. The internalization of ITGC/ITAC is an important path to the integration of fundamental IT governance knowledge within corporate assets, and it allows the auditor to become a proficient catalyst of knowledge. This is especially true when the auditor follows the entire audit process, including the basic and important evaluation of IT controls. There are no particular reasons to outsource IT controls except for the lack of knowledge or expertise. However, every cloud has a silver lining, and internalization of knowledge, in this case, could be an investment in increased professionalism rather than in not-so-proficient outsourcing.

REFERENCES
ISACA, CISA® Review Manual 2010, USA, 2010
ITGI, IT Assurance Guide: Using COBIT®, USA, 2007
ITGI, IT Control Objectives for Sarbanes-Oxley, 2nd Edition, USA, 2006
KPMG; Geneva & Université Zürich Institut für Rechnungswesen und Controlling “Objectifs de Contrôle Pour l’Information et les Technologies Associées (COBIT),” 2005
Laudon, Ken; Jane Laudon; Management of Information Systems, Prentice Hall, USA, 2006