

## Internal Audit of an Information Technology (IT) Services Business—An Overview



*The IT industry comprises of companies which provide services and solutions to cater to the IT needs of its customers. Considering the current technological world where we live in, this effectively means that companies or organisations in every other industry are potential customers for the IT industry. This fact clearly indicates the enormity of the playing field for 'IT' companies to compete and deliver. Some of the typical services provided by IT companies relate to development and maintenance of applications, software support, management of clients' IT infrastructure, management of outsourced business processes, etc. So, if a typical internal auditor is asked to audit the service business, where would he/she start from? What are the key components of the business to be reviewed? How does one define and segregate the audit universe? Does a typical internal auditor really have the capabilities to audit the inherent complexities of the IT business?*

*This article attempts to answer the above questions by providing an overview of the components and key processes, the key risks and challenges in auditing a typical IT services business. Read on...*

The processes, sub-processes, key risks and focus areas would differ between companies and also within the same company based on their operating model, volume of business, core competencies, customer requirements and geographical presence. However, the following sections try to provide a highly simplified view to aid internal auditors in understanding some key concepts of a typical

business selling services and plan their approach accordingly.

### Key Lifecycle Phases and Process Components

The IT services business is a contract-driven business, typified by multi-year contracts between the service providers and the clients. The typical lifecycle of the business model follows the below given broad phases:

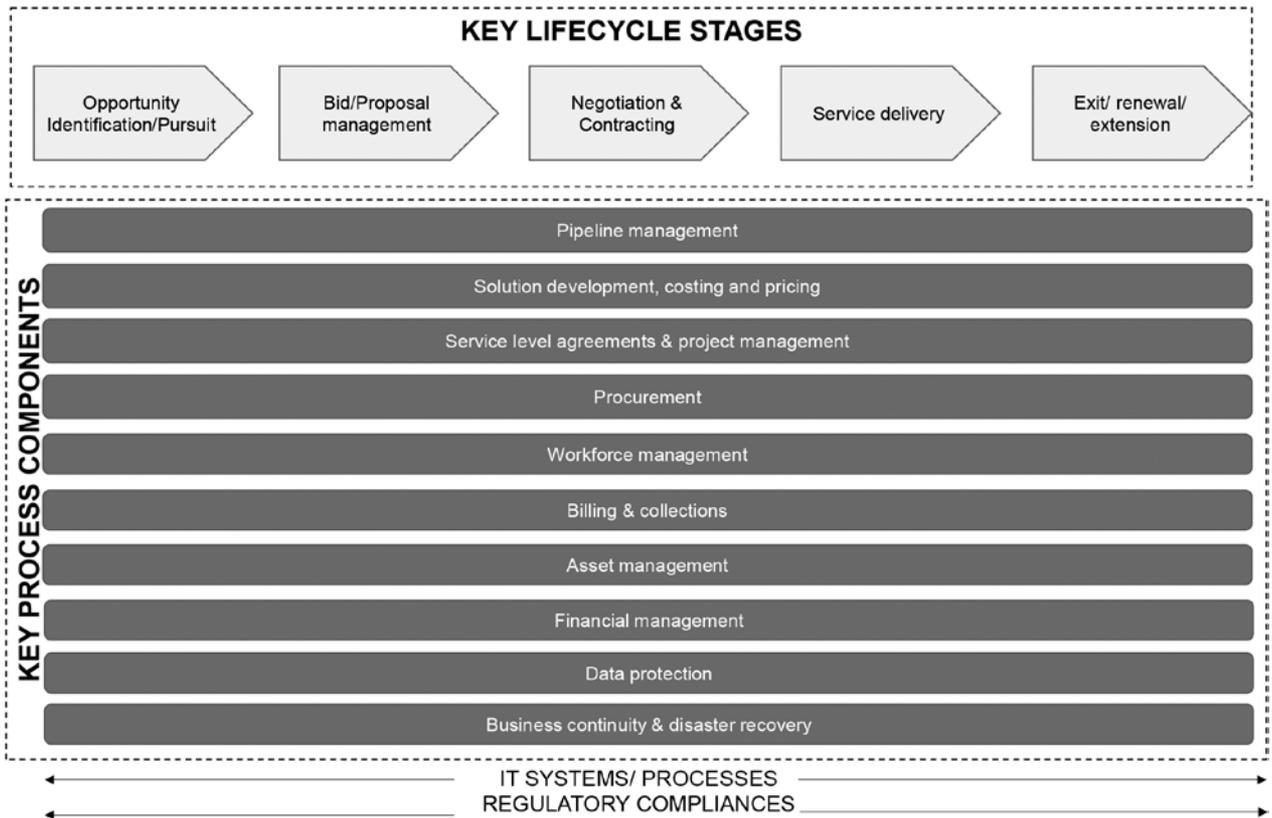
- Opportunity identification/pursuit
- Bid and proposal management
- Negotiation and contracting
- Service delivery
- Exit/renewal/extension



**CA. Parikshith Acharya**

(The author is a member of the Institute who may be contacted at [caparik@gmail.com](mailto:caparik@gmail.com).)

The following diagram provides an overview of the key lifecycle phases and the process components of a typical IT services business:



## Key Risk Elements for Focus

Now that we have got an overview of the key components, let us take a look at some of the key risk elements to be focused upon by an internal auditor. This has been depicted in the following table, for ease of reference:

#	Process component	Key risk focus elements
1.	Pipeline management	<ul style="list-style-type: none"> <li>• Demand generation and opportunity identification</li> <li>• Opportunity tracking, validation and qualification</li> <li>• Opportunity ageing and status monitoring</li> </ul>
2.	Solution development, costing and pricing	<ul style="list-style-type: none"> <li>• Technical solution development and review</li> <li>• Cost modelling assumptions and calculation</li> <li>• Price modelling</li> </ul>
3.	Service levels and project management	<ul style="list-style-type: none"> <li>• Definition of clear, measurable service level agreements (SLAs) for delivery and key performance indicators (KPIs)</li> <li>• SLA monitoring and reporting</li> <li>• SLA penalties</li> <li>• Penalty flow-down terms with third party sub-contractors</li> <li>• Maintaining customer relationship and obtaining feedback</li> <li>• Project start-up and ongoing delivery-scoping, monitoring and tracking</li> <li>• Project delays and cost overruns monitoring</li> </ul>

# Auditing

#	Process component	Key risk focus elements
4.	Procurement	<ul style="list-style-type: none"> <li>• Vendor qualification and selection</li> <li>• Negotiation and contracting, purchase orders/ statements of work (SOW) management</li> <li>• Vendor invoice processing and payments</li> </ul>
5.	Workforce management	<ul style="list-style-type: none"> <li>• Resource planning and hiring</li> <li>• Labour mix strategy (offshore/onshore, contract workers)</li> <li>• Labour demand-supply matching</li> <li>• Workforce training</li> <li>• Resource utilisation monitoring</li> <li>• Bench management</li> </ul>
6.	Billing and collections	<ul style="list-style-type: none"> <li>• Contractual billing schedules</li> <li>• Timely and accurate invoicing to clients</li> <li>• Legal entity billing model and related tax/regulatory compliances</li> <li>• Aged/disputed receivables and collections management</li> <li>• Provisioning for bad and doubtful debts</li> </ul>
7.	Financial management	<ul style="list-style-type: none"> <li>• Budgeting and forecasting</li> <li>• Revenue recognition, cost accounting and deferrals</li> <li>• Accruals accounting</li> <li>• Variance analysis</li> </ul>
8.	Asset management	<ul style="list-style-type: none"> <li>• Asset takeover, purchases per contractual schedules</li> <li>• Asset acquisition, leasing and disposal</li> <li>• Asset accounting (capitalisation, depreciation) and tracking</li> <li>• Physical verification</li> </ul>
9.	Data protection	<ul style="list-style-type: none"> <li>• Customer and employee data protection and confidentiality</li> <li>• Personally identifiable information protection</li> <li>• Cross-border data sharing regulations</li> </ul>
10.	Business continuity and disaster recovery	<ul style="list-style-type: none"> <li>• Existence and effectiveness of business continuity plans (BCP) and disaster recovery plans (DRPs)</li> <li>• Contractual provisions for BCP and DRP</li> </ul>

A couple of elements that need to be considered when reviewing each of the above process components and risk areas are as follows:

- *IT systems, processes and controls:* This is a common thread that runs through all of the above components and an auditor should evaluate the impact of IT systems and controls on each of the above process components and their output. For instance, the auditor should:
  - o assess the dependency of processes such as procurement, delivery (incident management, problem management, SLA tracking), labor supply/demand matching, billing, financial management, *etc.* on the respective IT systems used therein;
  - o assess the existence and effectiveness of IT general controls as well as the application controls inbuilt in the above systems, which could be critical to mitigate risks to the effective functioning of the business process.
- *Regulatory compliance:* This is another key factor to be kept in mind when auditing the above process components and all the more so for companies which operate in multiple geographies. For instance, the business units have to assess and ensure that there are controls to comply with various laws that may be applicable to:
  - o the regular employees and contract workforce (labour laws)

- o data protection and privacy laws
- o accounting regulations
- o local tax laws and foreign exchange regulations applicable based on the billing model
- o transfer pricing regulations applicable to inter-company cross-charges.

### Challenges before the Auditor

Auditing a services business with so many inherent complexities and across multiple locations does pose a lot of challenges. Some of the key challenges and points to ponder could be as follows:

- **How does one assess and prioritise the key risks that matter?**

Internal auditors should assess and prioritise key risks to the business objectives. This can be achieved through a mix of own prior experience and judgment, keeping pace with developments in the industry, leveraging relationships with other governance and compliance organisations (such as ERM, other compliance groups), risk input discussions with senior management of the business units, implementing self-assessments and data analytics.

- **What should be the approach to address and cover these risks? Should the auditor perform audits for each individual customer contract or for 'horizontal' processes across contracts?**

There is, obviously, no single or simple answer for this. The IT services business is a contract-based business; hence it may make sense to audit operations of each individual contract/account, especially for the high-value contracts. However, materiality considerations and structure of the organisation (centralised/decentralised) should also be kept in mind when deciding on the approach. Also, remedial actions may need to be taken across contracts to mitigate common control deficiencies, which might be more feasible to drive by performing 'horizontal' process-level audits across multiple contracts.

- **Should audits be performed to cover operations at each country where the company operates in or at a sub-region or regional or the global level?**

The answer to this question will be similar to as that of the above. There cannot be a 'one size fits

**The IT services business is a contract-based business; hence it may make sense to audit operations of each individual contract/account, especially for the high-value contracts. However, materiality considerations and structure of the organisation (centralised/decentralised) should also be kept in mind when deciding on the approach.**

all' solution, the approach needs to be finalised based on the unique conditions and environment the company operates in. The ideal approach is to adopt a mix of various approaches—standalone contract audits, process-level audits at the country or regional levels and governance audits at the global level.

- **Does the audit team have the desired levels of competence and skill sets to audit the risks of the services business, considering the inherent technological complexities?**

Adequate amounts of training—on-the-job, classroom and self-study is a prerequisite for any internal auditor, which should serve the purpose here too. It also helps to have a mix of auditors in the team with relevant, varied experiences and backgrounds such as strong career auditors, members rotating from business units, auditors with more finance acumen as well as ones with more operations or technical background. For instance, internal auditors may not always be able to assess the technicalities of complex solutions. However, they can and should be able to logically understand the processes risks and controls/governance processes around solutions development, and accordingly comment on the design and effectiveness of the control environment.

### To Conclude

The headwinds in the IT industry are firmly headed towards the latest concepts of providing services on the 'Cloud' and 'Big Data' analytics. This indicates more interesting times ahead for internal auditors since they need, more than ever before, to keep up with the latest developments in the IT services business arena and understand the changing risk landscape and accordingly tailor their approaches to provide assurance to all stakeholders. ■