A survey conducted in 2008 among audit committee members and auditors reporting to audit committees indicated that information technology, in itself, was not a key issue that audit committees could address. What was key was business, the uses business made of technology, the threats and risks associated with those uses, and the steps taken to mitigate those risks. The survey indicated that audit committees focused on business issues and treated technology as an enabler in business processes. A common theme was, “Do not tell me what controls are not effective; tell me what business process may be compromised, what business processes I cannot rely on, and their potential impacts if I do not address the risk.” In other words, the IT audit and assurance professional must become more business-focused.

That business focus may lead the IT audit and assurance professional into additional areas that encompass enterprise strategy, culture and goals, and the role that information technology plays in supporting these and other enterprise initiatives. Knowledge of business strategy, enterprise mission and goals, and monitoring objectives and key milestones, including effective measurement and benchmarking, may assist IT audit and assurance professionals in focusing their audit to better meet management’s and board of directors’ expectations.

Granted, the IT audit or IT review will focus primarily on technology-related business risks. However, to be effective, IT audit and assurance professionals must report their observations and findings in business terms. In other words, they must write for their audience.

That may be easier said than done. IT audit and assurance professionals require deep technical knowledge to scope the assignment, conduct the assignment, assess the findings, and develop workable and effective recommendations in technology-complex environments.

IT audit and assurance professionals have attained certifications, such as the Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM), that demonstrate their knowledge and competence in IT audit and control as well as security management. These professionals are well recognized and appreciated for their technical knowledge and skill, but could they be more valuable to the enterprise?

The issue then becomes one of providing IT audit and assurance professionals with training in business—in other words, training that includes knowledge of key business processes, how businesses are organized, the environments in which they work, and the issues facing businesses in remaining compliant with an ever-increasing plethora of laws, regulations, rules, standards, industry guidelines and other requirements.

This article explores the rationale behind the drive to equip IT audit and assurance professionals with increased business skills and an increased understanding of the enterprise and how it operates. It addresses the pros and cons, as well as the issues that management, the general auditor, and the IT audit and assurance professional may raise. It presents a business case for expanding the business knowledge and role of the IT audit and assurance professional and how to get started with this business-oriented mind-set.

ESTABLISHING GOALS

Ultimately, IT audit and assurance professionals must be comfortable presenting technology-related business risks and their potential impacts to boards of directors, executive management and other stakeholders. Presenting technology issues in a business context ensures that management is better informed and better able to understand the risks, issues, implications and impacts when making technology-related business decisions.

Accordingly, IT audit and assurance professionals should have the skills to understand underlying business processes, which will enable them to convey their technical findings with a business focus.

Robert G. Parker, CA•CISA, CMC, FCA, a retired Deloitte & Touche partner, is a past international president of ISACA and currently serves on the ISACA Frameworks Committee, the AICPA-CICA Privacy Task Force, the CICA Information Technology Assurance Committee and the Board of the University of Waterloo Centre for Information Systems Assurance. Parker is the primary architect of ISACA’s Information Technology Assurance Framework (ITAF). He is a frequent author and speaker on information security, control, risk management and privacy issues—areas in which he practices.
Relevant Business Knowledge

Business knowledge encompasses an understanding of businesses—what the business is—including legal status, organization, governance, structure, culture, risk tolerance or appetite, operations, and uses of technology in providing services to business units. Further, it includes what the business does, including products, services, markets, customers and users—in other words, an understanding of the business from the perspectives of different stakeholders.

It also includes knowledge of the business and industry environments, the governing laws and regulations, and the policies and procedures designed to encourage and enforce compliance. It involves an understanding of industry trends and best practices. It requires that the IT audit and assurance professional understand operational, financial, accounting and reporting systems and their uses within the enterprise.

Knowledge and understanding of business information can help IT audit and assurance professionals better assess the impact of any identified risks and findings and communicate these in terms that are relevant and understandable to boards of directors, executives, senior and line management, and others who may not possess a detailed understanding of technology and its potential impact on the business. For example, there may be a lower tolerance for risk in publicly traded and/or highly regulated businesses than in privately held businesses. Accordingly, the IT audit and assurance professional’s business knowledge will assist them in developing relevant and practical recommendations that add value to the business.

Impact of Business Knowledge on an IT Audit

Greater business knowledge will likely increase the relevance and practicality of IT audit findings and recommendations, in that they will address business impacts in terms that can be understood and assessed by management and others not possessing a detailed understanding of technology. Rather than indicate that a control is missing or ineffective, the IT audit and assurance professional with appropriate business knowledge and skills should also identify the business impact, such as “shipping will not be possible” or “we may be in contravention of privacy laws,” and quantify the risk in terms of the likely financial, reputational, legal or other impacts.

Improved findings and recommendations will increase the value of IT audit and assurance assignments to the business units, executive management and boards of directors by providing better and more effective decision-making information.

Audit committees tend to consider IT an integral component of business processes and deal with it as such. Accordingly, IT audit and assurance professionals possessing increased business knowledge will be able to discuss issues and impacts in terms that members of boards of directors can better comprehend and address.

Boards of directors need to understand the risks, mitigating initiatives being undertaken and any residual risks when dealing with core business processes. Further, when business strategy dictates changes, such as outsourcing, developing major systems or changing technologies, the IT audit and assurance professional will be better able to relate these in business, rather than technical, terms to the board of directors and senior management.
EIGHT BUSINESS KNOWLEDGE AREAS

Businesses maintain significant amounts of information that encompass business intelligence, knowledge of business processes, procedures and standards, knowledge of products and services, and information on markets and competition. With this wide range of information, the first task is to determine what business knowledge is relevant to IT audit and assurance professionals.

For ease of discussion, eight categories of business knowledge that IT audit and assurance professionals need to understand are defined:

- How is the enterprise organized?
- How is the enterprise governed?
- Under what laws/regulations does the enterprise operate?
- What are the enterprise’s business processes?
- How does the enterprise operate?
- How does the enterprise use technology?
- How does the enterprise finance itself?
- How does the enterprise measure business success?

The IT audit and assurance professional should understand the basic principles of business: planning, acquiring assets and other resources, producing goods or delivering services, evaluating performance, and determining how these principles relate to the business. In addition, there will likely be a need to acquire additional industry-specific knowledge, particularly in those industries in which procedures have become well recognized and adopted or are required by legislation, regulation, industry-adopted standards or legal agreement.

IT audit and assurance professionals should gain an understanding of the industry in which the enterprise operates. First, they should classify the enterprise into one of the 11 categories identified in figure 2. Industry knowledge serves to put organizational initiatives, changes, strategies and plans into context. It helps the IT audit and assurance professional comprehend the rationale for some of management’s decisions and the key external drivers.

Understanding the size and complexity of the enterprise, the multijurisdictional aspects of its business, and the specific audit and assurance requirements will increase the effectiveness of IT audit and assurance professionals, the work they perform and the usefulness of the resulting reports.

Figure 2—Enterprise Classifications

<table>
<thead>
<tr>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services (e.g., banks, investment firms, insurance companies)</td>
</tr>
<tr>
<td>Consumer-intensive (e.g., retail stores, direct marketing, service businesses, entertainment, hospitality)</td>
</tr>
<tr>
<td>Health care (e.g., hospitals, health care providers, clinicians, technology providers, health insurance providers)</td>
</tr>
<tr>
<td>Transportation (e.g., airlines, trucking, coastal and deep-sea shipping, railways)</td>
</tr>
<tr>
<td>Government (e.g., federal, state/provincial, municipal and local, related boards and agencies)</td>
</tr>
<tr>
<td>Resource industries (e.g., oil and gas, mining, forestry, exploration, extractions)</td>
</tr>
<tr>
<td>Manufacturing (heavy and light industries)</td>
</tr>
<tr>
<td>Extractive (e.g., energy, mining, agriculture, fishing)</td>
</tr>
<tr>
<td>Utilities (e.g., hydroelectric, nuclear, coal generation, solar, wind turbines, tidal, gas distribution)</td>
</tr>
<tr>
<td>Public sector (e.g., federal, subfederal and local government, public agencies and corporations, public education, military)</td>
</tr>
<tr>
<td>Nonprofit organizations (e.g., associations, charities, foundations)</td>
</tr>
</tbody>
</table>

ORGANIZATION

The IT audit and assurance professional should understand the differences in the types of enterprises—how they are created, what legal authority they are given, and their reporting and filing obligations. This would involve gaining an understanding of the different forms of enterprises, such as limited liability companies, public vs. private companies, multijurisdictional, foreign, and parent vs. subsidiary, as well as other forms such as partnerships, proprietorships, joint ventures and nonprofits.

Understanding the size and complexity of the enterprise, the multijurisdictional aspects of its business, and the specific audit and assurance requirements will increase the effectiveness of IT audit and assurance professionals, the work they perform and the usefulness of the resulting reports.

GOVERNANCE

The IT audit and assurance professional should understand the governance structure and governance processes—including the enterprise’s organization and where each business unit and supporting function fits within the enterprise’s structure—as well as the lines of authority and reporting. In addition, the audit and assurance professional should have a firm grasp of the roles and responsibilities of each level of management, where these are defined, for example, in position descriptions and job/committee charters; how they are operationalized; and how compliance is monitored.
This would involve gaining an understanding of the enterprise’s governance processes from an enterprise perspective, including board of directors, executive and line management, and technology. Further, it would involve gaining an understanding of the roles and responsibilities at various levels throughout the enterprise and how the various roles contribute to an effective governance process. Additionally, an understanding of governance will require gaining an understanding of the enterprise’s policies, procedures, standards, practices, guidelines, directives and other information that establishes the operating infrastructure of the enterprise, as well as an understanding of the accountability and reporting structure. Finally, the IT audit and assurance professional should understand the enterprise’s risk appetite—how it monitors, assesses and addresses risk and how it deals with uncertainty.

LAWS AND REGULATIONS
Legislation, regulations and rules play an important role in structuring the enterprise’s business processes and practices by providing guidance and direction, as well as requiring compliance. By understanding the legislative and regulatory requirements and their impact on the business processes, the IT audit and assurance professional is better able to appreciate the boundaries placed around the enterprise’s operations and the requirements to comply with various rules and regulations.

The IT audit and assurance professional must also consider compliance requirements when scoping audit, assurance and advisory assignments. Failure to understand and consider the legal implications could make the IT audit and assurance professional’s work less relevant or even inaccurate or unusable.

BUSINESS PROCESSES
IT audit and assurance professionals should understand the day-to-day business processes inherent in any business. They should comprehend the physical activities involved in each business process, as well as the information acquired, documented and used in that process. Further, they should understand the flow of that information throughout each process and the controls over the information to ensure its integrity.

Core business processes include acquiring resources, making products, marketing and selling products or services, collecting money, and reinvesting in the enterprise’s core processes. In addition, the IT audit and assurance professional should understand the enterprise’s process for monitoring and controls established to ensure appropriate performance. Core business activities could also include research and development, as well as methodology and software design and development to enable the enterprise to improve existing products and services or develop new ones.

The IT audit and assurance professional should also understand the other business processes in which the enterprise engages. While these are not core business activities, they are required to sustain the enterprise. These include securing capital, financing operations, recruiting and managing staff, computing and paying taxes, and other supporting activities.

As previously indicated, the IT audit and assurance professional will likely encounter situations that require increased knowledge of external environments, such as industry standards or technical requirements, legislative and regulatory obligations, and their impact on the enterprise’s business processes.

OPERATIONS
The IT audit and assurance professional should understand basic business models—such as the ConT model of Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate; or the ISO model (based on the Deming cycle) of Plan, Do, Check, Act—that can be applied to an enterprise’s operations.

Further, IT audit and assurance professionals should relate the models to their own enterprises to understand their enterprises’ business life cycles. In doing so, they should identify key process documentation used in monitoring and controlling operations and the key reports relied upon by management to monitor and evaluate these processes.

Key operational processes may include inventory, manufacturing, sales/order entry, purchasing, payroll, receivables and collections in a manufacturing entity. In the hospitality industry, it may include designing tours, consolidating vendors and managing vacation packages, or arranging entertainment and marketing events.
The IT audit and assurance professional should also gain an understanding of any industry-specific requirements that influence the business process through legal, regulatory, industry-mandated or other criteria. The IT audit and assurance professional should understand not only what is happening throughout the business cycle, but also why it is happening and how it is being performed, including how it is being controlled and reported.

**USE OF TECHNOLOGY**

Enterprises adopt and use technology differently. The degree to which they use technology, the business processes supported or led by technology, and the approaches and means of minimizing technology risks while leveraging technology gains will impact the IT audit and assurance professional's approach to an assignment and, accordingly, the knowledge and skills required.

**Figure 3** illustrates three stages in the business use of technology: support, enabler and business-centric. Technology used to support business processes is the basic level, and may involve typical financial and administrative processes. At the enabler level, the business is using technology to extend business processes to achieve greater efficiency, effectiveness or cost savings. At the business-centric level, the use of technology is an integral and critical component of the entire business, for example, an e-commerce business.

By using the table in **Figure 3** as a means of classifying the business use of technology, the IT audit and assurance professional can determine the sophistication of the technology environment and the knowledge and skills required to conduct an effective audit.

**FINANCIAL**

Financial information, whether developed for regulatory or statutory reporting or for managing specific operational and business processes, is a critical element of any business. Financial information must not only be complete, accurate and timely, but must also be relevant, in that it meets the users' needs and allows them to appropriately manage the business.

IT audit and assurance professionals should understand the "flow of the numbers," just as they should understand the physical flow of goods and the corresponding flow of information involved in each business process. This will require a basic knowledge of accounting—the debits and credits, and the accounting for each business process.

The IT audit and assurance professional should also understand the methods and rationale for recording financial transactions within each business process, such as sales, deferred sales, product development costs and amortization of product costs. Further, the IT audit and assurance professional should understand various accounting processes that record costs, such as standard cost, job cost and process cost methods of accounting for manufacturing processes, as well as the treatments of overheads.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Function</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>IT is used to assist selective business processes; however, those processes can easily and effectively be performed manually.</td>
<td>IT supports the business process.</td>
<td>Residential service business (e.g., home painting, cleaning), in which IT is used to maintain customer lists, scheduled dates and maintain basic financial information</td>
</tr>
<tr>
<td>Enabler</td>
<td>IT is used to enable the operation of a business process that may be impractical without the use of technology.</td>
<td>IT enables the business to extend the business process.</td>
<td>Retail organization using point-of-sale (POS) registers, SKUed inventory control and integrated financial systems</td>
</tr>
<tr>
<td>Business-centric</td>
<td>IT is the business. The business model is conceived around an IT solution.</td>
<td>The business could not operate and would not function without IT.</td>
<td>Web operations, such as eBay and Amazon, or business-specific, such as AMR-Saber reservation system</td>
</tr>
</tbody>
</table>
The IT audit and assurance professional should also understand how basic business accounting results in three types of reports:

- **Financial reporting**—Allows the enterprise to comply with statutory reporting requirements, such as quarterly and annual filings with stock exchanges
- **Regulatory reporting**—Such as to taxation authorities, utility regulators, or insurance and financial regulators, allows the enterprise to demonstrate compliance with specific requirements
- **Operational reporting**—Provides senior management, supervisors and line managers with information to control business processes, as well as to report various operational information to senior and executive management

**BUSINESS MEASUREMENTS**

Every business needs a method to measure progress and accomplishments. IT audit and assurance professionals should understand the fundamentals of establishing business goals, strategies and plans. They should also understand the various ways to measure progress and attainment of business goals throughout the enterprise, and how to roll these up for executive and board reporting.

Knowledge and skill in measurement techniques, such as return on investment, net present values, discounted net present value, payback period and discounted cash flow, to name a few, are required to ensure that the information being provided to management is appropriate and relevant for the business purpose.

Knowledge and competency in these eight areas will provide IT audit and assurance professionals with a solid foundation of business processes to enable them to deal with technical issues from a business context and to communicate observations, findings and analyses, and develop effective recommendations for boards of directors, executives, and senior and line management.

**GETTING STARTED**

There are a number of considerations to be addressed prior to embarking on a program to provide IT audit and assurance professionals with business knowledge and training. They include:

- The individuals' current level of business knowledge and skill
- The anticipated use that the individuals will make of the business information and skills obtained
- The type of work to be conducted and the degree to which that work will require and/or benefit from increased business knowledge and skill
- The culture within the enterprise with respect to education and training
- The structure of the department or area in which the IT audit and assurance professionals work and its relationship with the board of directors and executive management, for example, the reporting protocols and meeting attendance requirements

These business skills are in addition to the other skills required by the IT audit and assurance professionals, including communications, relationship management, interview, analytical, and dealing with resistance and difficult situations.

While many enterprises will welcome the additional business knowledge and skills possessed by the IT audit and assurance professionals, others may see it differently. Such skills may well suit IT audit and assurance professionals in providing advisory services, more than those performing technical tasks in support of a compliance audit team.

Entities should consider carefully the purpose and rationale of equipping IT audit and assurance professionals with increased business knowledge and skills. Providing education and training to equip IT audit specialists with business skills that may never be used, or that will detract from their other skill sets, may prove to be detrimental to the individuals' careers and the enterprise's management of their expectations. Conversely, keeping IT audit and assurance professionals in technical roles that limit their ability to master new skills and grow within the enterprise will likely be equally detrimental.

Accordingly, each situation must be carefully weighed and a balance must be obtained.

**ISSUES AND CONCERNS TO BE ADDRESSED**

Identifying the issues to be overcome in ensuring that IT audit and assurance professionals are fully equipped with appropriate business knowledge will require that they not only understand the issues, but also how to address effectively any risks or deficiencies through recommendations that are logical, practicable and business-focused.

Issues and concerns to be addressed include:

- **Technology focus**—Potential IT auditors recruited from a technology/computer science background may lack even basic business knowledge and skills. Their strengths may
lie more in the area of technology than in business and, accordingly, they may thrive on the technology more than the business issues and may not want to dilute their highly focused technical skills.

- **Resources and time**—Enterprises may lack the time, talent, and financial and other resources to add business knowledge and skills to the knowledge base of their technically focused IT auditors.

- **Team concept**—IT audit departments and, in particular, general audit departments may operate on a team basis, with general auditors providing the business knowledge and the IT auditors providing their technical skills to the general audit team, thus limiting the IT audit and assurance professional’s overall involvement in the business aspects of the audit. Additionally, IT audit reports may be drafted by technical IT audit and assurance professionals, but edited and presented by the general auditor, thereby limiting the need for the IT auditor to “speak business.”

- **Specialization**—IT audit and assurance professionals may focus on one particular technology, business unit or business process, and, accordingly, management may be concerned that the IT audit and assurance professionals would not have an opportunity to use the additional business skills.

- **IT audit and assurance professional’s career**—A number of IT audit and assurance professionals may want to be involved only in the “techie” side of IT audit and assurance work and may not naturally gravitate to the business issues.

- **General auditor perception**—The general auditor may have a perception of the IT audit and assurance professionals as only technology specialists. Therefore, the IT audit and assurance specialists may not be invited to key meetings or may be precluded from participating in the business communications process, thereby limiting the perceived need for, and opportunity to engage in, business-focused discussions.

- **Executive and management perception**—Executive and management may be unwilling to entertain the idea of increasing the IT audit and assurance professional’s knowledge or expanding the IT audit and assurance professional’s role.

- **Expectations of IT audit and assurance specialists**—The expectations of management and others may vary; they may consider “IT audit” to consist of three roles:
  - IT audit control specialist (e.g., security, control, privacy)
  - IT audit technical specialist (hardware/software)
  - IT audit systems/application development specialist

  A lot of the focus may be on the development specialist as a value-add in supporting an enterprise’s systems development projects, with less focus on the very technical hardware or software IT audit specialists’ role.

Conversely, with the increased importance of security, controls and privacy, management may prize the IT audit role in supporting its controls reporting. A lack of clarity or frequent shifts in the enterprise’s expectations of IT audit and assurance specialists may either encourage or stifle the IT audit and assurance specialist’s ability to obtain business knowledge and skills.

Given that the enterprise can successfully address the issues and concerns and can develop a career path for IT audit and assurance professionals that includes the continued and increasing effective use of their business and technical skills, developing individual career paths, including an increasing business focus, would appear appropriate. This will involve assessing current business skills, identifying appropriate sources of training, ensuring that training is provided and that the IT audit and assurance professional is progressing, and developing the appropriate skills for use within the enterprise.

**ACQUIRING BUSINESS SKILLS**

There is no shortage of places where business knowledge is available. There is no shortage of people willing to teach business skills. However, finding the right combination that allows the IT audit and assurance professional to acquire the appropriate knowledge and the skills to use that knowledge effectively within an audit, assurance or advisory role can be difficult.

While continuing education seminars and courses, executive or part-time business degrees, training weeks, and retreats are ready sources of business information, their cost and time commitment may not be affordable or warranted in all cases.
Other sources such as industry groups, night school courses and certificate programs should be considered. Businesses themselves can create opportunities for IT audit and assurance professionals to acquire business skills—through job shadowing, job rotation and mentoring programs.

CONCLUDING THOUGHTS
IT audit and assurance professionals bring considerable technical skills to audit, assurance and advisory assignments. Their participation provides additional insight, a technical perspective and identification of technical issues, concerns, problems and solutions to any assignment. Their participation increases the effectiveness of the assignment by including technology-related risks and threats, increased insight into potential causes and impacts, and heightened awareness of the pervasiveness of technology in most business processes.

With technology embedded in most business processes and with reliance on technology being critical, the lines between business processes and technology processes are becoming blurred.

Does it still make sense to treat IT audit and assurance work as a separate component of audit and assurance assignments? Would it not be better to equip IT audit and assurance specialists with business skills to allow them to more fully understand all of the business issues and impacts and provide them with the skills to communicate effectively with boards of directors and executive management?

Providing IT audit and assurance professionals with increased skills to enable them to assess the business, as well as the technical aspects of an issue, would benefit both the professional in terms of career satisfaction and also the enterprise in terms of the quality and relevance of the analyses performed and the recommendations made.