An ISACA
Cloud Computing Vision Series
White Paper
February 2012

Trust in, and value from, information systems

Guiding Principles for Cloud Computing Adoption and Use

Abstract

The drive for value, the need to reduce technology costs and the business demand for increased agility in how technology is used have caused enterprises to adopt cloud computing strategies. These strategies leverage the infrastructure, platforms or software services provided by cloud providers, transferring information technology (IT) from an in-house service to an outsourced capability. While enterprises have experience with the technology that makes cloud possible, and have used IT outsourcing to control costs or to enhance service levels, they have less experience transferring IT decision making away from the chief information officer (CIO) and technology specialists and to business unit leaders. Cloud represents a fundamental shift in how technology is acquired and managed in enterprises. This shift can result in pressure on the enterprise when its structure, culture, policies and practices, and enterprise architecture have not evolved to address the changes inherent in the cloud computing shift. This paper describes the nature of cloud computing and areas of pressure that, when not addressed, can increase risk to the enterprise. It also presents six principles for cloud computing adoption and use that can guide management toward more effective cloud implementation and use, reduction of pressure points, and mitigation of potential risk.

ISACA®

With 95,000 constituents in 160 countries, ISACA is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA has designed and created *Guiding Principles for Cloud Computing Adoption and Use* (the "Work") primarily as an educational resource for security, governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security, governance and assurance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Guiding Principles for Cloud Computing Adoption and Use

Acknowledgments

ISACA wishes to recognize:

Contributors

Ramses Gallego, CISM, CGEIT, CCSK, CISSO, CISSP, SCPM, 6 Sigma, Quest Software, Spain, Chairman
Assaf Afek-Levy, CISA, CRISC, CISSP, Aviva, Canada
Abhishek Agarwal, CRISC, CIPP, Kraft Foods, USA
James Arlen, CISA CRISC, Push The Stack Consulting, Canada
Gautam Basu, CISA, CAIIB, OCP, MCP, State Bank of India, India
Roberth Chavez Jara, CISA, Deloitte, Ecuador
Chintan Chawla, CGEIT, India
Vilmos Csuri, CISA, CISM, CGEIT, CRISC, ITIL-F, Hungarian Post Pte Ltd., Hungary
Chandresh Dedhia, Ratnakar Bank Ltd., India
Stefano Ferroni, CISM, Beta 80 Group, Italy
Sailesh Gadia, CISA, CA, CIPP, CPA, KPMG LLP, USA
Vicki Gatewood, CGEIT, CRISC, USA
Nigel Hedges, CISA, CISM, CISSP, Kaspersky Lab Australia and New Zealand, Australia
Mamane Ibrahim, CISA, CRISC, APMC, CMQ/OE, PMP, Michelen, France
Hussam Khattab, CISA, MCSE, PMP, Arab Bank PLC, Jordan
Masatoshi Kajimoto, CISA, CRISC, Japan
Valdez Ladd, CISA, CISSP, Siemens Medical Solutions Inc., USA
Yves Le Roux, CISM, CISSP, CA Technologies, France
Marco Aurelio Maia, CRISC, PMP, Modulo Security Solutions S.A., Brazil
Henry Maphosa, CISA, TransAlta Corporation, Canada
Grace McEwen, CISA, USA
Bassil Mohammad, CISA, CISM, CRISC, CEH, LISA, Ernst & Young, Jordan
Adityan Murthy, CISA, CRISC, PMP, Abu Dhabi Commercial Bank, United Arab Emirates
Harry Neilson, CISA, GSNA, ICM, United Kingdom
Amar Padmanabha, CISA, CCSK, USA
Eric Phifer, CISA, CRISC, CTGA, MCSE, Seacoast National Bank, USA
Bill Powell, CGEIT, ITSM, Zenetex, USA
Ramesan Ramani, CISM, CGEIT, Paramount Computer Systems, United Arab Emirates
Antonio Ramos García, CISA, CISM, CGEIT, ITIL, Leet Security and n+1 Intelligence & Research, Spain
Martin Rohrer, CISM, CRISC, Bank Julius Baer, Switzerland
Mandar Sahasrabudhe, CISA, CISM, KPIT Cummins Infosystems Ltd., India
Amr Said, CISA, CISM, CRISC, Nokie Siemens Networks, Egypt
Martin M. Samson, CISM, CGEIT, CRISC, Nurun, Canada
Jose M. Fidel Santiago Luque, CISA, CISM, Belgium
Dandeelo Siena, CISA CISM, Security+, ITIL V3, JP Morgan Chase and Co., Philippines
Arun Sondhi, CISA, ITIL, PMP, Six Sigma, Accenture LLP, USA
Vikrant Tanksale, CISA, ACWA, CMA, Al Bahja Industrial Holdings LLC, Sultanate of Oman
Daniel Venere, Cardif Compañía de Seguros Generales S.A., Chile
Jasmin Wai Mun Loh, CISA, CIA, FCCA, Singapore Management University, Singapore
Michael Yung, CISA, CISM, Next Media Limited, Hong Kong

Special Recognition

ISACA New Jersey Chapter for its financial support

Acknowledgments *(cont.)*

ISACA Board of Directors

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired) USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President
Lynn Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

Knowledge Board

Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, USA
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

Guidance and Practices Committee

Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
Ramses Gallego, CISM, CGEIT, CCSK, CISSO, CISSP, SCPM, 6 Sigma, Quest Software, Spain
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Yongdeok Kim, CISA, IBM Korea Inc., Korea
Perry Menezes, CISM, CRISC, Deutsche Bank, USA
Mario Micallef, CGEIT, CPAA, FIA, Advisory in GRC, Malta
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico
Nikolaos Zacharopoulos, CISA, CISSP, Geniki Bank, Greece

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors

American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association (ISSA)
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
GRC Solutions Inc.
Hewlett-Packard
IBM
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

The Cloud Computing Challenge

Cloud computing references abound in business and technical circles. Yet, for all its current pervasiveness, there is still an ongoing debate as to what cloud is and how it should be addressed by technology, risk management, compliance, security, assurance and business unit leaders. Contributing to the difficulty is the fact that definitions have focused on what cloud providers deliver in terms of technical infrastructures, platforms or complete, ready-to-use services, instead of what cloud is.

Definitions also tend to present cloud computing in terms of location and ownership: internal to the enterprise, delivered through the efforts of an external service or infrastructure provider, or as a hybrid public-private solution. For each type of cloud (infrastructure, platform or software service) and for each arrangement (public, private or hybrid), the challenges presented and the management approach required can be very different. The strategic value that cloud computing brings to an enterprise and the operational and technical types of risk that need to be considered differ across each possible deployment style. How cloud solutions are managed, the controls required and the necessary level of vigilance in terms of monitoring and reporting can also vary significantly depending on the type, location and nature of cloud solution ownership. The challenge is to understand the value that cloud computing represents to the enterprise and how this value can be achieved by effectively governing and managing cloud computing as a component of the enterprise IT strategy.

This paper presents a generally accepted definition of cloud computing as a basis for describing it, but also offers additional views of what it is based on, how it is being used and the value it promises to provide. The differences between cloud computing and traditional means of providing information system services to support enterprises are presented, and areas of organizational pressure that these differences can cause are explored. Finally, guiding principles for effective, pressure-free cloud computing adoption and use are presented. These principles describe important considerations that business management and those responsible for ensuring the protection of information and business processes must address when selecting or implementing a cloud solution. The appendix describes additional guidance from ISACA that addresses the need for enterprises to develop approaches to cloud computing that will help ensure that cloud infrastructure, platform or software services will provide expected business value.

Definition, Values and Benefits

It is important to understand what cloud computing is and what separates cloud from other forms of IT and service delivery methods. The differences that make cloud computing unique are also the things that enterprises hope to leverage to drive value, reduce costs, improve service levels and support constituents and customers. Understanding what cloud is makes evident the need to achieve balance between opportunity and risk.

The differences that make cloud computing unique are also the things that enterprises hope to leverage to drive value, reduce costs, improve service levels and support constituents and customers.

Enterprises already have significant experience with traditional approaches to information systems technology, IT service delivery and outsourcing. Guidance and good practice information is available for enterprises wishing to achieve optimal results from information systems or to more effectively manage outsourcing. Cloud computing is different, and those differences can create pressure points within the enterprise.

Pressure points are created when differences in the cloud do not quite align with organizational structures, decision making, culture, approaches to quality management, or aspects of protecting information and information processes. While many publications address technical and operational types of risk associated with cloud computing, pressure points are often overlooked. The differences in how enterprises need to govern, manage, implement and manage cloud infrastructures, platforms and services (as opposed to traditional approaches) need to be understood and accommodated if enterprises hope to extract maximum value from cloud solutions and trust these solutions to protect sensitive and private information and reduce the likelihood or impact of security and other incidents.

Formal Definition

The most widely accepted definition of cloud computing has been released by the US National Institute of Standards and Technology (NIST). NIST describes cloud computing as:

> *a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction*[1]

The essential characteristics of cloud computing (and what distinguishes it) are its on-demand nature and its provision through broad network access to a shared pool of resources, where use can be expanded or retracted as needed and cost is based on use. These essential characteristics apply regardless of whether the cloud is provisioned as an infrastructure, platform or software service offering, or as an internal, external or hybrid implementation. Virtualization, while an important aspect of cloud computing, is not cloud computing if characteristics such as Internet-based access and elastic scalability are not part of the implementation.

While the NIST definition effectively lays out the essential characteristics of cloud computing, it describes only what cloud computing is in its most basic form. It does not address the equally important aspects of how cloud computing is used within enterprises or how it differs from other technology solutions and delivery mechanisms. The pressure points that enterprises need to consider and plan for are more easily identified within the context of how cloud is used, what the business drivers are, and how cloud as a business technology solution is different from traditional computing delivery approaches. Understanding the pressure points better prepares enterprises to more effectively govern and manage internally and externally provided cloud solutions and to integrate cloud as part of the overall business strategy.

Enterprise Values and Benefits

The formal definition of cloud computing and its essential characteristics provides key insight into the cloud. Equally important is an understanding of its values and benefits. These drive its adoption and use, whether as the dominant information systems strategy or as a supplement to technology services during times of peak demand. Understanding the values and benefits, as well as the essential characteristics, is necessary to define where pressure points may exist and how the enterprise can respond to them.

The benefits of agility, cost containment, multitenancy, reliability and scalability have been associated with cloud computing.

The benefits of agility, cost containment, multitenancy, reliability and scalability have been associated with cloud computing as follows:

- **Agility**—Enterprises move at the speed of the Internet. The time from inception to general acceptance of technologies, and from concept to fully implemented solution, has shrunk from decades to years and continues to decrease. Agile enterprises understand that markets move quickly and being first to market is a powerful advantage. The ability to deploy technologies, build innovative system solutions and meet customer needs has become a decisive capability. Quickly adopting better, more market-responsive solutions, while avoiding solution lock-in enables agile enterprises to maximize investments and market opportunities. Cloud infrastructures and platforms, or ready-made software solutions, provide a level of agility not easily matched by non-cloud solutions.
- **Cost containment**—Cloud computing can enable enterprises to use financial resources for maximum impact. Traditional in-house technology solutions can require a substantial capital investment for facilities and technology acquisition. Costs for cloud, on the other hand, are operational in nature. Once an organizational need is identified, the operational capabilities can be acquired from infrastructure, platform or software service providers meeting the short-, intermediate- or long-term needs of the department or user group. Public cloud provides technology without capital investment. Due to the on-demand nature of cloud services, capacity requirements to support organizational technology needs for periods of peak demand are not a consideration. Capital investments in data centers and

[1] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing: Special Publication 800-145*, 2011, *www.nist.gov/itl/cloud/*

technology infrastructures require planning for periods of peak consumption, resulting in technology deployments that are underutilized during normal periods of demand. Leveraging cloud to support capacity requirements and balance utilization across platforms reduces capital requirements, making funds available for operational and high return-on-investment opportunities.

- **Multitenancy**—The shared nature of cloud computing distributes costs and capabilities among a wider group of users. Because cloud computing is an externally provided service offering, the multitenant aspect enables not only the sharing of technical infrastructures and applications, but also the specialized expertise of technology workers. Cloud infrastructure, platform and service providers can afford to invest in world-class solutions because the cost is shared among many subscribers. Investment in the development and management of information system solutions within the cloud environment should produce solutions that are not only more economical, but also more effective, efficient, secure and resilient.
- **Reliability**—The essential characteristics of cloud computing, including broad network access to a shared pool of resources and rapid elasticity based on need, enhance the reliability of cloud solutions—a reliability enhanced by the entrance of large international technology providers into the cloud market and the virtualization of their infrastructures. Technology providers who offer infrastructure, platform or software service solutions can be expected to deliver a large, well-managed, internationally deployed solution base to support tenant requirements regardless of location. The technical sophistication of the cloud architecture as implemented by providers, the cloud's geographic dispersion, its duplication of data and applications across locations, and the ability to instantaneously switch data stores and applications to other servers across multiple locations can create a solution that is highly resistant to outages and service interruptions.
- **Scalability**—Cloud computing has the potential to serve the needs of small and medium enterprises as well as governments and *Fortune* 100 corporations. Each enterprise can determine its unique needs and find a solution that will deliver value, from the cloud's provisioning of infrastructure and development platforms to software as a service (SaaS). Small and medium enterprises, and particular start-up ventures, may select to leverage infrastructures, platforms and services. Larger enterprises may need only to supplement their existing information system capabilities by leveraging infrastructures to address specific nonroutine needs or to incorporate mobile applications more quickly into their application portfolios. SaaS providers may leverage infrastructure and platform capabilities available in the cloud to take advantage of ready-made solutions so they can focus on their core capability—innovation in service development. The ease with which service levels can be expanded/reduced and the pay-for-what-you-use nature of cloud computing make cloud computing particularly scalable to the needs of tenants.

The business needs that drive enterprises to consider cloud computing, cloud's essential characteristics, and the values and benefits that are expected from it form a more comprehensive picture of cloud and its relation to organizations. This information is necessary to identify what is different about cloud computing—differences that create pressure points that need to be identified and managed. An understanding of how cloud computing is regarded within the enterprise and the relationship of cloud solutions to overall organizational strategy contributes to effective governance and management of cloud solutions.

This information is necessary to identify what is different about cloud computing—differences that create pressure points that need to be identified and managed.

Pressure Points

Within the space where cloud computing differs from internally provided IT services or outsourced arrangements, potential pressure points exist. These pressure points result from changes in technology or the use of technology, changes that may require management to consider the impact these differences have on how technology acquisition and use is governed, managed, monitored and controlled. Subtle differences in cloud computing—such as the change in cost allocation from capital expenditures to operational expenses—may have consequences that are not immediately apparent. Because cloud acquisitions for infrastructure, platform or software services are an operational rather than capital expenditure and have a lower cost of entry, decisions about those acquisitions may fall outside of traditional review and approval processes. Important governance and risk management triggers that in other circumstances would result in management oversight and review may not occur. Operational risk related to the geographic distribution of data, issues related to joint tenancy and compliance, contingency and continuity planning, and many other factors may not come to the attention of those within the enterprise who need to integrate cloud solution planning into the overall approach for compliance and risk management. Pressure points do not necessarily represent risk to the enterprise. They represent areas that need to be identified so that enterprises can trust the cloud computing solutions they depend on and receive the value that cloud computing is expected to bring.

Speed and Agility

Enterprises that depend on the Internet need to move at the speed of the Internet. The speed-to-market driver for technology acquisition and adoption makes cloud computing a suitable strategy for enterprises hoping for first-mover advantage. Cloud's fast and easy availability means that technology is not the market differentiator it has been in the past—technical infrastructure is simply a means to an organizational end.

> **The speed-to-market driver for technology acquisition and adoption makes cloud computing a suitable strategy for enterprises hoping for first-mover advantage.**

The description of cloud computing as a utility results from the pressured time-to-market driver. Solutions to meet market needs can be more economically developed and delivered more quickly if enterprises can leverage ready-made development platforms or acquire software services from a cloud provider. Having an application that is strategically conceived and meets exact organizational requirements may not be as important as having applications available that can be deployed for mobile users or to support specific needs.

The agile exploitation of technical solutions to achieve strategic objectives in reduced time frames puts greater pressure on enterprises in which culture, process and human factors related to technology have been developed to support longer development cycles and longer-term use of technology solutions. Without a commensurate change in organizational culture, processes and procedures, and effective integration of human factors into technical solutions, these areas of high pressure can increase the potential for risk related to the following outcomes:

- An unbalanced prioritization of value over trust in technology solution choices
- Missed opportunities when other alternatives are not considered
- Recovery mishaps because fallback positions are not fully explored
- Missing functionality if full requirements are not identified
- Increased long-term costs due to reliance on multiple short-lived solutions
- Reduced performance when enterprises are hesitant to introduce new solutions because of existing technology investments

Changing Boundaries

As enterprises rely on technology to reach out to markets, the barrier between the enterprise and its external environment evaporates. Outsourcing and reliance on third parties to provide technology services or to support organizational strategy further undermine this barrier, as does the pressure to meet mobile user needs and expectations to be protected when communicating with enterprises or using available application services. The reliance on cloud providers can change roles and responsibilities within enterprises. Where once software services had been developed, deployed and supported by internal parties, outsourcing and other third-party arrangements transfer certain responsibilities to outside parties. Contracts and service level agreements (SLAs) with external providers attempt to assign accountabilities, but governance dictates that enterprises themselves, their boards and management remain accountable. Cloud computing may disrupt assigned responsibilities as the locus of decision making changes from governance functions such as compliance, risk management, security and assurance, to business line leaders. Traditional governance processes and those who are responsible for the governance of information and IT may not be informed or consulted as decisions to leverage cloud solutions are being made. Monitoring and reporting to support oversight and control may not be incorporated into cloud solutions as they would with other technology strategies.

Changes in organizational boundaries and internal and external roles and responsibilities can put greater pressure on enterprises. Organizational structure, processes and procedures, and roles and responsibilities need to be aligned to ensure that the value expected from cloud services is obtained and cloud services can be trusted. Not addressing expanding internal and external organizational boundaries can result in areas of high pressure and the following risk outcomes:

- Role confusion when accountabilities and responsibilities are not clearly defined
- Diminished effectiveness when decisions are made without engaging in a wider consideration of trust and value before cloud platforms, infrastructure or software services are acquired
- Failure to satisfy constituent and end-user expectations for protection and privacy
- Project delay and increased costs due to the need for personnel with governance responsibilities to revisit cloud plans
- Unclear specifications of provider responsibilities and accountabilities in SLAs
- Incomplete information being provided to board members and senior management

Organizational structure, processes and procedures, and roles and responsibilities need to be aligned to ensure that the value expected from cloud services is obtained and cloud services can be trusted.

New Technologies and Technology Expectations

Cloud computing has been described as a disruptive technology. Its disruptive nature results from the convergence of computing technology, communication capabilities, and approaches to application development and their impact on the business use of technology. From an evolutionary standpoint, cloud computing has become possible as a result of the transition through the different epochs of computing: from mainframe dominance, to the introduction of workstations and personal computing, to the introduction of mobile devices and tablets. Each trend in computing has brought new opportunities for enterprises to prosper and has caused them to reconsider how technology is governed and integrated into their core processes. Cloud follows a sequence of disruptions in how technology is viewed, integrated into organizational strategy and managed within the enterprise, and in how technology-related business risk is identified and managed.

The introduction of new technologies may apply pressure on enterprises in which enterprise architectures have evolved primarily to address internally provided and managed technology solutions, human factors related to the use of technology have been developed to facilitate use of traditional computing devices by insiders, and the enablement of process and support for technology are defined for internally controlled infrastructures and applications. Areas of high pressure can result when organizational strategy and enterprise architecture do not consider the unique qualities of cloud computing, or when human factors related to information systems do not include mobile devices and tablets. Pressure may result when enterprise processes and procedures do not easily adapt to changes made possible by cloud computing or where cloud solutions do not make processes and procedures more effective and efficient. These areas of high pressure can result in the following risk outcomes:

- Missed opportunities to extract value from the integration of cloud and internal information systems
- Increased vulnerability from incompatibilities and inconsistencies between cloud solutions and internal information systems
- Less-than-expected results when human factors are not considered in the design and integration of cloud services and infrastructures
- Levels of organizational performance that do not meet expectations because cloud solutions do not fully support organizational processes
- Levels of technical performance that do not meet expectations because processes do not take full advantage of cloud capabilities

Pressure may result when enterprise processes and procedures do not easily adapt to changes made possible by cloud computing or where cloud solutions do not make processes and procedures more effective and efficient.

Level Playing Field

Cloud computing removes the advantage that large enterprises have traditionally had in terms of the availability of technology specialists and technical sophistication. Small and medium enterprises that take advantage of infrastructure providers to support technology needs and provide specialized platforms for development and testing can build an innovative infrastructure capable of enabling entry into a global marketplace with as much capability as the market demands. Smaller enterprises have the ability to leverage software services that provide customer relationship management and business analytics, traditionally available only to large enterprises. Being able to access infrastructures, platforms and software services based on what is needed and paying for only what is used empowers start-up enterprises and small and medium enterprises, giving them an advantage in the market and an equal position with much larger enterprises.

This leveling of the playing field can put pressure on enterprises that do not recognize the impact cloud computing can have when developing or implementing their strategies. Pressure can also result when the organizational culture is not open to emergent market opportunities that are best addressed by leveraging cloud solutions. Not considering the strategy implications of cloud computing on existing and new market opportunities can result in areas of high pressure and the following risk outcomes:

- New entrants claiming a segment of traditional market dominance
- Strategies that do not address competitor capabilities
- Less-than-expected benefits received from technology-dependent solutions

This leveling of the playing field can put pressure on enterprises that do not recognize the impact cloud computing can have when developing or implementing their strategies.

Utility Services and Service Supply Chains

Enterprises have traditionally extracted value from ownership of technology and systems. This value may be reduced in a market in which technology and systems can be instantly acquired, expanded or contracted based on need; development and management costs are shared among a large base of users; and cost is directly associated with resources used. In an environment in which computing is a technology utility, there is less concern for how the infrastructure, platform or software services are developed. More focus is paid to organizational needs, expected benefits to be delivered and the value that can be obtained from the computing utility.

The agile enterprise benefits from solutions that can be used as needed and discarded when they no longer provide value. Those enterprises are sensitive to market opportunities and leverage supply infrastructures, platforms and software services, creating a value supply chain that can be reconfigured as needs and market conditions change.

The view of computing as a utility and the delivery of cloud solutions as a supply chain of information system solutions puts greater pressure on enterprises that contain a culture that is not accepting of utility solutions, a structure that does not facilitate cooperative planning and integration of utility solutions, and processes that cannot take advantage of computing solutions provided as a supply chain of utilities. Enterprises that fail to consider the impacts of cloud solutions seen as a computing utility brought together into a supply chain of IT capabilities may experience areas of pressure resulting in the following risk outcomes:

- Overinvestment of resources in planning and building internally developed information system solutions
- Less-than-optimal results when value-producing cloud utilities are missing from the total solution
- Duplication of effort when specialist services available through cloud providers are not integrated as part of system management
- Less-than-expected results when utility components are not integrated into and managed as an information system capability supply chain

Guiding Principles for Cloud Computing Adoption and Use

The technical nature of cloud computing, the way it is delivered and deployed, and the benefits it promises can lead to areas of pressure on the enterprise that can result in inefficiencies and less-than-effective use of both internal and cloud-provided solutions. In more extreme cases, areas of pressure can result in operational risk and incidents that can have more significant consequences. To obtain value from cloud computing, cloud infrastructures, platforms and software services need to be trusted. To meet organizational goals, cloud strategies and solutions need to be integrated with internally provided technology strategies and solutions. Value and trust, as well as effectiveness and efficiency, can be obtained when cloud solutions are included within the governance and management structures of the enterprise and management follows the guiding principles of practice as outlined in the next section.

The technical nature of cloud computing, the way it is delivered and deployed, and the benefits it promises can lead to areas of pressure on the enterprise that can result in inefficiencies and less-than-effective use of both internal and cloud-provided solutions.

Guiding Principles

Cloud computing represents an evolution in how enterprises acquire and use technology and interact with and support internal and external users and customers. Because of its evolutionary nature, clear guidance is lacking in setting a direction for executive management or those responsible for determining how cloud will be used and how it fits within the organizational structure and processes. With further evolution will come better understanding, bringing more specific guidance addressing the legal, operational and technical types of risk. Such guidance will help reduce the need to plan for building trust to achieve value at each step in the acquisition and integration of cloud solutions.

To help illuminate a path for enterprises, ISACA has provided the following guiding principles for cloud computing adoption and use. It is too early in the life cycle of cloud computing to propose strict rules for the adoption and use of cloud infrastructures, platforms or software services; however, principles that provide prudent boundaries of behavior or describe a basic quality of trust or value applicable to cloud computing will help support decision making that will, in turn, reduce pressures and control risk.

The six guiding principles for adopting and using the cloud are enablement, cost benefit, enterprise risk, capability, accountability and trust:

- **Enablement principle**—Plan for cloud computing as a strategic enabler rather than as an outsourcing arrangement or a technical platform. The drivers for cloud computing are strategically oriented. The agility that cloud promises to enterprises, the ability to contain and transfer technology costs from a capital expense to an operational expense, leveraging the benefit of paying for what is used when it is needed, and resource sharing among multiple subscribers provide capabilities that, while operational, enhance the ability of enterprises to enter new markets, better meet customer expectations and conserve resources. Enterprises that approach the cloud from a purely technical perspective may miss many advantages that cloud computing can provide. Viewing it as a replacement for internal technology solutions limits the ability of enterprises to think broadly about how it can support the strategic direction of the enterprise. A limited technical perspective will not tend to lead to the examination of the organizational structure, governing processes, enterprise architecture and culture. These aspects of how technology is embedded into business processes can engender later consequences in the form of organizational pressure resulting from cloud adoption.

  To plan strategically for cloud adoption and use, enterprises need to:
  - Treat cloud computing adoption and use as a strategic business decision.
  - Make informed decisions, considering both business and operational needs and the benefits that can be provided by cloud computing.

The six guiding principles for adopting and using the cloud are:
- **Enablement**
- **Cost benefit**
- **Enterprise risk**
- **Capability**
- **Accountability**
- **Trust**

- – Communicate cloud computing arrangements and agreements to internal parties to ensure proper alignment and consistent oversight.
- – Periodically review organizational strategies and the contribution of IT to ensure that cloud initiatives maximize value delivery, risk management and resource utilization.

- **Cost benefit principle**—Evaluate the benefits of cloud acquisition based on a full understanding of the cost of cloud compared with other technology platform business solutions. The full cost of provisioning technology infrastructures and services is much larger than the cost of facilities, hardware, software and the annual cost of human resources. The full cost of acquiring and deploying cloud infrastructures, platforms or software services is more than what is represented within the cloud contract and SLA. Enterprises must also make substantial investment in the governing structures, processes and procedures, enterprise architectures and culture required to make technology and applications an essential element in how the business is managed and how internal and external value is assured. Investments must be made in people and their skills, and in professional certifications that demonstrate their competencies.

  The true cost of cloud computing needs to be measured against the total investment and ongoing costs of providing similar services using internal resources. The investment in people, process and technology creates a value structure that may not be easily replicated within the context of a cloud service strategy.

  To properly evaluate the costs and benefits of cloud computing, enterprises need to:
  - – Clearly document expected benefits in terms of rapid resource provisioning, scalability, capacity, continuity and the cost reductions that the cloud services offer.
  - – Define the true life-cycle cost of IT services provided internally or through a provider to have a basis for comparing expected and received value.
  - – Balance cost with functionality, resilience, resource utilization and business value.
  - – Look beyond cost savings by considering the full benefits of what cloud services and support can provide.
  - – Periodically evaluate performance against expectations.

- **Enterprise risk principle**—Take an enterprise risk management perspective to manage the adoption and use of cloud.

  Guidance concerning cloud-related risk has focused on technical aspects related to virtualization; the possible exposure of sensitive information within a shared environment; issues related to compliance and, in particular, privacy regulations and the export of personal information; and legal issues involving SLAs. Although these represent issues with which organizational management should be concerned, addressing each as a separate risk may not be productive and may not reduce the risk exposure of the enterprise. Decisions about cloud infrastructures, platforms and software services that are based on a series of what seem to be independent types of risk may not result in the best risk management. Instead, examining risk within the context of an enterprise approach that incorporates technical and operational risk will help management understand the cumulative impact of a separate cloud risk.

  A consolidated examination of risk and risk impacts can help management understand the actions needed to mitigate and control risk or to make prudent decisions about what risk can be accepted. Completing a scenario analysis that combines the multiple facets of risk—including business, legal, reputation, compliance and technical considerations—will help management understand the enterprise's true position, which will help in making valid decisions about the extent of risk associated with cloud as compared to other technology and infrastructure solutions.

  To understand the risk implications of cloud computing, enterprises need to:
  - – Consider the privacy implications of comingling data within the virtualized computing environment.
  - – Evaluate privacy requirements and legal restrictions, considering client needs as well as provider restrictions and capabilities.
  - – Determine the accountability addressed in SLAs, the ability to monitor performance and available remedies.

  - Understand current risk identification and management practices and how they need to be adapted to address risk management for cloud computing.
  - Integrate scenario analysis into business risk management decision making.
  - Consider exit strategy and the implications of not being able to render data as enterprise applications are sunset or unavailable.
- **Capability principle**—Integrate the full extent of capabilities that cloud providers offer with internal resources to provide a comprehensive technical support and delivery solution. Cloud computing promises to enhance the technical capabilities of enterprises. Resource sharing in a multitenant infrastructure enables tenants who independently may not be able to make the investment for the newest technology solutions or to create the redundancy necessary to provide 100 percent availability. Resource constraints have caused enterprises to attempt to do more with fewer resources, or to plan for redundancy only for the most critical devices, potentially leaving the enterprise vulnerable to denial-of-service attacks or at risk to outages resulting from device failure. In addition to a resilient and extensible technical architecture, cloud providers offer other benefits such as human resources, including individuals with specialized skills or personnel available on a 24/7 basis, which may otherwise have been outside the tenant's reach.

  Technology and people come together in an environment in which policies and processes, as well as tools and performance aids, contribute to the ability of cloud suppliers to deliver exceptional levels of service to tenants. The advantages that result from sharing technical, human and other resources may not automatically benefit tenants. To gain the full advantage, enterprises need to understand the resource capabilities they possess as well as the resources that the supplier makes available. Understanding what capabilities are offered and how they can be combined with internal resources, and developing a plan to leverage these combined resources, will set apart those enterprises that achieve exceptional results.

  To leverage both internal and cloud provider resources effectively, enterprises need to:
  - Understand the human and technical resource capabilities that exist in the current infrastructure and how a cloud strategy will impact the need for these or other resources.
  - Define the capabilities that a cloud provider will make available as well as constraints on these resources, including periods of unavailability or priority of use.
  - Consider emergency situations and resource requirements necessary to determine causes, stabilize the environment, protect sensitive and private information, and restore service levels.
  - Determine how policies, practices and processes currently support the use of technology; how transitioning to a cloud solution will require policy, practice and process changes; and the impact these changes will have on capabilities.
  - Ensure that service providers can demonstrate that personnel understand information security requirements and are capable of discharging their protection responsibilities.
  - Ensure that internal staff have the skill and expertise to coordinate activities with cloud providers and that they are engaged in cloud service acquisition and ongoing management.
  - Ensure that effective channels of communication are provided with provider management and key specialists, particularly for problem identification and resolution.
- **Accountability principle**—Manage accountabilities by clearly defining internal and provider responsibilities. Enterprises that govern IT effectively, clearly define responsibilities and enforce accountabilities. Within this principle, all aspects of technology design, implementation, testing, use by business units and specific responsibilities for essential actions are defined and individual groups are held accountable for decisions, actions or the failure to perform. Organizational structures provide a mechanism for institutionalizing responsibilities, while policies, practices and procedures provide a mechanism for implementing controls that enforce accountabilities. When enterprises move to a cloud solution, there is a shift in the organizational structure that can have significant consequences on how accountabilities and responsibilities are implemented. Adopting cloud solutions may break connections among people, technology, the processes that enable technology use, and the enforcement of individual and group accountabilities and responsibilities.

To ensure that responsibilities are clearly understood and individuals and groups can be held accountable, enterprises need to:

– Understand how traditional responsibilities are assigned and implemented within the existing organizational structure and as a part of policies and practices to determine how these are addressed within cloud solutions.
– Determine how responsibilities between tenant and provider organizations for cloud solutions are assigned and how communications between accountable individuals and groups will be facilitated.
– Ensure that processes and procedures provide a mechanism to ensure that responsibilities are accepted and accountabilities are clearly assigned.
– Maintain within the governance structure a means of reviewing performance and enforcing accountabilities.
– Consider the risk to the enterprise as part of the enterprise risk management program, the impact of potential lapses in assigned responsibilities, or the impact of not being able to assign accountabilities.

- **Trust principle**—Make trust an essential element of cloud solutions, building trust into all business processes that depend on cloud computing. Capturing the desired value from cloud strategies requires trust to be established. Trust is evident when the user believes that private information in a cloud application remains private and outcomes expected from the use of an application will be realized. Trust is an essential requirement for business applications of technology for internal and external users. It results from the combined effect of organizational structure, culture, technical architectures, processes and the human factors that facilitate the deployment and use of technology in support of business functions.

Enterprises rely on security personnel to build controls that ensure that private and sensitive information remains confidential, that information flows and processes have integrity, and that essential information systems and the information they depend on are available when needed. Audit personnel provide assurance that the policies and processes defined to ensure the confidentiality, integrity and availability of information and information systems are effectively implemented and information and business process risk is identified and managed. The combination of security, risk management and assurance services ensures that business management, internal users and external parties can trust that information systems provide the expected value. Trust for cloud computing solutions incorporates the combined effect of tenant and provider security, risk management, and assurance plans and activities. To achieve trust, these efforts need to be coordinated.

To ensure that business processes that depend on cloud computing can be trusted, enterprises need to:

– Clearly define confidentiality, integrity and availability requirements for information and business processes.
– Understand how reliance on cloud computing solutions may impact trust requirements.
– Structure the efforts of security, risk management and assurance professionals within both tenant and provider organizations to ensure that trust requirements are known and satisfied.
– Monitor changes in business use of cloud computing, vulnerabilities associated with cloud solutions, and implementations across tenant and supplier environments to ensure that threats to trust can be identified and resolved.
– Ensure that cloud infrastructure, platform and software service providers understand the importance of trust and create solutions that can be trusted.
– Provide ongoing assurance that information and information systems can be trusted.

Conclusion

Cloud computing presents a unique opportunity for enterprises. Gaining its intended benefits means that enterprises must consider it as a component of organizational strategy, as a cost model, as a component of enterprise risk management, and as a delivery mechanism that supports organizational goals and objectives. Effective decision making about its value to the enterprise and its integration into the business fabric require that cloud computing be incorporated into the governance, risk management, and service delivery plans and activities of the enterprise. The six principles outlined in this section have been developed to address emerging issues and concerns relative to cloud computing, provide guidance that will help enterprises achieve the benefits they expect from cloud solutions, and ensure that internal and external users can trust these solutions.

The business and functional perspectives of the governance of enterprise IT are as important for the use of cloud computing solutions as they are for the use of technology. The business perspective is necessary to ensure that technology and systems support and enable the business. The functional perspective ensures that technology use is effective and efficient, that effective governance promotes the optimal use of technology and system resources, that risk management balances opportunity and risk, and that value is created for the enterprise.

The business perspective is necessary to ensure that technology and systems support and enable the business. The functional perspective ensures that technology use is effective and efficient, that effective governance promotes the optimal use of technology and system resources, that risk management balances opportunity and risk, and that value is created for the enterprise.

Additional Resources and Feedback
Visit *www.isaca.org/cloud-principles* for additional resources and use the feedback function to provide your comments and suggestions on this document. Your feedback is a very important element in the development of ISACA guidance for its constituents and is greatly appreciated.

Appendix. ISACA Cloud Computing Resources

Enterprises take advantage of cloud offerings to increase the value that IT and information systems bring. Realizing value from the cloud requires that decisions be made considering costs and risk, and with a view of cloud solutions as part of the portfolio of technology offerings in support of the organizational strategy. Val IT, an ISACA governance framework available at *www.isaca.org/valit*, provides guidance to executives and those charged with making decisions concerning the use of technology in support of organizational objectives. The guidance contained in Val IT is appropriate for informing decision making relative to cloud computing.

Additional guidance for boards and executives is contained in the *Board Briefing on IT Governance, 2nd Edition*, which is available at *www.isaca.org/boardbriefing*. While this briefing was originally intended to address the need to govern traditional IT investments and deployments, the adoption of cloud computing may have increased the need for effective governance because of the need to rely on a third party for services that can significantly impact value delivery, risk management and the achievement of strategic organizational goals.

Cloud computing potentially can present challenges in terms of risk that needs to be identified and pressure points that need to be evaluated before they increase risk to the enterprise. The risk related to cloud computing that management needs to consider extends beyond the purely technical aspects of virtualization or the issues associated with reliance on a third-party service provider. Cloud offers enterprises the business advantage resulting from more agile development and delivery of IT, the ability to contain costs, resource sharing among cotenants, the reliability that cloud infrastructures can provide, and the scalability of solutions. The need to balance these expected rewards with potential legal, reputational and operational types of risk requires that management integrate cloud risk management into a larger program for managing business risk related to the use of IT. ISACA's Risk IT framework, available at *www.isaca.org/riskit*, provides a structure for managing risk that addresses diverse aspects of business risk, including project risk, value delivery, compliance, misalignment of cloud with strategy requirements, and service delivery.

The Business Model for Information Security (BMIS), available at *www.isaca.org/bmis*, provides a model that presents the interconnections between the enterprise and the people, processes and technologies that enterprises use to provide business value. This systemic view of security helps to clarify how the culture of the enterprise, human factors, the enterprise architecture and emerging conditions can be a force for enabling value from cloud solutions or a detractor in achieving organizational objectives. The interplay of elements (such as people, process and technology) and dynamic forces within enterprises can create pressure points that reduce the utility of cloud solutions or enhance the value obtained.

ISACA has also developed more specific guidance for cloud computing adoption and use. This includes an introduction to cloud issues and strategies in *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, and more specific guidance in *IT Control Objectives for Cloud Computing*, available at *www.isaca.org/cloud*.

The ability of enterprises to obtain value from the use of technology is a fundamental cloud computing challenge. Cloud represents a change in how departments obtain the platform, infrastructure or software services that are required to operate more effectively, reach customers or expand the business to new markets. To gain the expected benefits, enterprises need to consider how cloud impacts and is impacted by the cultural, technical and human aspects of the enterprise, as well as how the governing structures and procedures enable the use of cloud technology. COBIT, an IT governance and management framework, with supporting tool sets, helps enterprises bridge the gap between business needs and technical solution implementations and management. COBIT and its related products, available from ISACA at *www.isaca.org/cobit*, identify essential processes and associated management guidelines required in planning, acquiring, supporting and monitoring technology solutions to ensure that essential business objectives are satisfied. The COBIT framework can be used for the governance and management of internal and supplier technology solutions, ensuring that business objectives are indentified, responsibilities and accountabilities are clearly indentified, and results meet business owner expectations.

A challenge in selecting a cloud solution provider is understanding the quality of services offered. Enterprises adopting cloud solutions need to understand not only the maturity of service that a provider is offering, but also how this maturity compares with processes currently offered internally that will be supported by the provider or integrated with provider capabilities. The COBIT Process Assessment Programme, based on COBIT 4.1 and available at *www.isaca.org/cobit-assessment-programme*, provides a standardized method of assessing the maturity of technology processes contained in COBIT using the methodology promoted in ISO/IEC 15504-2. The COBIT Process Assessment Programme provides a means of identifying the maturity of internally managed processes and evaluating these against service provider processes.

The adoption and use of cloud computing is evolving as enterprises gain experience in leveraging cloud infrastructures, platforms and software services. As cloud offerings are revised and improved to meet changing needs, business and technology leaders will need guidance to ensure that value can be obtained and trust can be assured. ISACA will continue to provide guidance and practice resources for information security, information systems assurance, and risk management and compliance professionals and their business unit counterparts. The ISACA Knowledge Center (*www.isaca.org*) provides a ready source of current information on cloud computing and other important topics, as well as a location for members to exchange views and share insights.