Cloud computing is gaining momentum. As cloud offerings gain maturity, cloud service providers are becoming more competitive. Some providers are reducing prices as they realize investments and leverage economies of scale. Others are differentiating based on quality, for example, providing better availability, improved security or enhanced ability to manage services. While the benefits of cloud computing are real in economic, strategic and operational terms, realizing those benefits is not a simple process. To achieve the benefits of cloud computing, adoption drivers must be aligned with enterprise goals and objectives, and business and cultural factors must be favorable for adoption. Like any investment, cloud projects should be guided by the board of directors to ensure value creation and optimization of risk. When evaluating cloud initiatives, board members should ask their management teams specific questions, the answers to which will determine whether cloud services will have a positive and sustainable impact on enterprise goals and whether risk remains within enterprise tolerances.
Cloud Governance: Questions Boards of Directors Need to Ask

Isaca

With more than 100,000 constituents in 180 countries, ISACA (www.isaca.org) 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 and expands the practical guidance and product family based on the COBIT® framework. COBIT 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 Cloud Governance: Questions Boards of Directors Need to Ask (the “Work”) primarily as an educational resource for 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 all 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, governance and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

© 2013 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

Cloud Governance: Questions Boards of Directors Need to Ask
ISACA Wishes to Recognize:

**ISACA Board of Directors**

**Gregory T. Grocholski,**
CISA, The Dow Chemical Co., USA, International President

**Allan Boardman,**
CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President

**Juan Luis Carselle,**
CISA, CGEIT, CRISC, Wal-Mart, Mexico, Vice President

**Christos K. Dimitriadis,**
Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President

**Ramses Gallego,**
CISM, CGEIT, COSK, CISSP, SCORM, Six Sigma Black Belt, Dell, Spain, Vice President

**Tony Hayes,**
CISM, CAFSE, CHE, FACTS, FCPA, RIA, Queensland Government, Australia, Vice President

**Jeff Spivey,**
CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President

**Marc Vael,**
Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Chairman

**Rosemary M. Amato,**
CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands

**Steven A. Babb,**
CGEIT, CRISC, Belfair, UK

**Thomas E. Barton,**
CISA, CISM, CRISC, CISSP, Cost Plus, USA

**Phil J. Lageschulte,**
CISM, CPA, KPMG LLP, USA

**Jamie Pasfield,**
CISM, ITL V3, MSP, PRINCE2, Pfizer, UK

**Salomon Rico,**
CISA, CISM, CGEIT, Deloitte LLP, Mexico

**Guidance and Practices Committee**

**Phil J. Lageschulte,**
CISM, CPA, KPMG LLP, USA, Chairman

**Dan Haley,**
CISA, CISM, CRISC, COP, Ernst & Young LLP, Johnson & Johnson, USA

**Yves Marcel Le Roux,**
CISM, CISSP, CA Technologies, France

**Aureo Monteiro Tavares Da Silva,**
CISM, CGEIT, Brazil

**Jotham Nyamari,**
CISA, Deloitte, USA

**Connie Lynn Spinelli,**
CISA, CRISC, CFE, CGMA, CIA, CISSP, CMA, CPA, BKD LLP, USA

**Siang Jun Julia Yeo,**
CISA, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore

**Nikolaos Zacharopoulos,**
CISA, CISSP, DeutschePost-DHL, Germany

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

- Information Security Forum
- Institute of Management Accountants Inc.
- ISACA chapters
- ITGI France
- ITGI Japan
- Norwich University
- Socitum Performance Management Group
- Solvay Brussels School of Economics and Management
- Strategic Technology Management Institute (STMI) of the National University of Singapore
- University of Antwerp Management School

- ASIS International
- Hewlett-Packard
- IBM
- Symantec Corp.
Introduction

Board members are hearing more and more from their management teams about the noteworthy business benefits of cloud computing, such as:

- **Cloud strategies make the enterprise more efficient and agile.**
- **Cloud computing allows delivered services to be more innovative and more competitive.**
- **Cloud computing reduces overall operating costs.**

But how confident can boards be that management plans will achieve these benefits? Is there a way to know that, even if the benefits are real, increased operational risk will not outweigh those benefits? Fortunately, by understanding what cloud is and what it is not and by asking a few key questions of management teams, boards can gain that confidence—in management plans and strategic goals, as well as in the decisions made in response to those plans.

This paper provides a brief overview of cloud computing and presents the important questions that board members should ask when evaluating cloud computing as part of their overall enterprise strategy. These questions serve as a starting point for opening conversations among executives, business line leaders and information technology (IT) management; they also serve as the foundation for building a common understanding of the expected benefits, allocation of resources and optimization strategies for any associated risk.
Value of Cloud Computing

The goal of cloud computing is to enable the enterprise to manage computing based on the financial, cultural or operational goals of the enterprise.

To understand the value of cloud computing, board members must first understand its purpose. The core goal of cloud computing is to turn enterprise computing into a fungible commodity. In the traditional model of IT, the enterprise acquires and maintains a portfolio of slowly depreciating technology assets that may or may not be employed efficiently. Conversely, the goal of cloud is to enable the enterprise to manage computing much like electricity, buying only what it uses (no more and no less). Another analogy is the decision that an enterprise makes whether to buy or lease physical office space. Both approaches have advantages and disadvantages, such as taxation considerations, predictability of costs, operational or capital expenditure and community and cultural factors. The decision is a choice—one the board makes based on the financial, cultural or operational goals of the enterprise. Cloud computing attempts to make the purchase and use of computing resources a similar choice based on similar parameters.

Because the underlying computing substrate of cloud computing can be dynamically replaced, provisioned or reallocated as needed, an enterprise can leverage competition among service providers to negotiate the best price, find the vendor that best supports the particular needs of the enterprise and rapidly incorporate new capabilities into its technology portfolio. This model can be applied to infrastructure-level computing resources (storage or networking), business applications or somewhere in between. By looking at cloud computing in this way, the board of directors can start to envision the possible benefits, for example:

- Shifting the funding of IT from large capital investments (legacy IT assets) to operational expenses.
- Reallocating IT resources to core business activities.
- Procuring applications that are easier and cheaper to implement, use and support.
- Increasing scalability and flexibility, enhancing the ability to respond to changing market conditions.
- Fostering innovation by shifting effort and resources from implementation projects to final product development.

From a technology standpoint, the components that make the cloud computing model possible are not new. It applies numerous technology advances that have been around for a long time: high-speed Internet access, server virtualization, new software development approaches, advances in high-capacity storage, etc. Cloud computing has implications outside of the traditional IT landscape. The impact of cloud computing extends throughout the enterprise. Its impact facilitates potential changes in enterprise culture and requires change in areas such as customer service, change management and vendor management to accommodate the unique qualities and requirements of cloud computing. An enterprise can leverage cloud computing to enhance the business model by facilitating the movement from brick and mortar to online services or extending market reach by removing geographic barriers. Cloud computing could be a disruptive enabler (a beneficial outcome that could require substantial changes) of business value and a means of providing technology services that are available more quickly and at a lower total cost.

The challenge is for board members to have sufficient understanding of the opportunity that cloud presents so that they can effectively direct and monitor plans to leverage cloud and promote success.
Governing Cloud Computing

Like any investment, cloud must be governed; however, some cloud computing characteristics (virtualization, agility, flexibility, faster deployment and minimal initial investment) may require additional governance considerations to ensure that benefits are realized within acceptable levels of risk.

Cloud services are often provided as metered services, much like the way consumers and enterprises purchase electricity. An enterprise can easily and quickly increase or decrease the service levels, based on fluctuating needs (need more, buy more). Within this model, individual business units can identify needs, negotiate contracts and implement services in a way that bypasses procurement processes that are required for proper governance. For example, Forrester estimates that for every cloud initiative tracked centrally by IT shops today, there are three to six initiatives that are not tracked.¹ Flexibility, or “pay-as-you-go,” enables a business unit to increase capacity or request additional services with a simple call. But there is a downside; this flexibility could also result in the bypassing of expense authorization, change control processes, information protection controls and other oversight processes.

Bypassing established governance processes and failing to inform others within the enterprise about cloud computing initiatives may result in the enterprise assuming unknown risk and, thereby, increasing potential exposure. Without close monitoring and proper discipline, cost overruns may result if services are not turned off when they are no longer needed. Individually purchased services may conflict with established technology strategies. In some instances, acquisition of cloud services resulted in regulatory problems—problems that could have been avoided if usage plans were communicated and systematically considered beforehand.

Governance Questions the Board of Directors Should Ask About Cloud

To establish a clear direction that is aligned with enterprise strategy, members of the board need to have a clear understanding of cloud computing benefits and how to maximize them through effective end-to-end governance practices. This requires the board to see cloud computing not as an IT project, but rather as a business technology strategy. This understanding helps to ensure that stakeholder needs are considered and met while risk and resource utilization are optimized.

The following questions help to identify the strategic value that cloud services may provide to the enterprise and the impact that cloud could have on enterprise resources and controls:

1. **Do management teams have a plan for cloud computing? Have they weighed value and opportunity costs?**
   The risk of cloud adoption may be inconsequential when compared to the lost opportunity to transform the enterprise with effective and strategic use of cloud computing. The loss can be particularly great when competitive enterprises take steps to leverage those same opportunities. From a strategic perspective, cloud computing can be a vehicle to:
   - Gain competitive advantage.
   - Reach new markets.
   - Improve existing products and services.
   - Retain existing customers.
   - Increase productivity.
   - Contain cost.
   - Develop products or services that could not be possible without cloud services.
   - Break geographic barriers.

2. **How do current cloud plans support the enterprise’s mission?**
   Cloud services should support efforts to achieve business objectives, which are derived from stakeholder needs (as vetted by the leadership team). Cloud initiatives should have a clear and traceable link to the enterprise strategy so that the value expected from cloud services is clearly defined, accepted and measurable. This link also helps to determine the priority assigned to cloud initiatives and supports the development of metrics to measure results against expectations.

   Alignment between cloud objectives and enterprise objectives is critical for effective risk management and cost containment. The potential benefits of cloud services can be enticing, but with reward comes risk. The enterprise must decide whether the potential risk is within acceptable limits.

3. **Have executive teams systematically evaluated organizational readiness?**
   Pressure points result when:
   - Cloud computing implementations conflict with enterprise culture.
   - Skills that are required to support cloud solutions are not available.
   - Cloud-related processes conflict with other established processes.
   - Organizational structure does not maximize cloud effectiveness or efficiency.
Evaluating the readiness of the enterprise in anticipation of the adoption of cloud services avoids the need for after-the-fact culture, skill or process changes to remove unanticipated pressure points. A systematic readiness assessment can help management identify additional cost and risk that should be factored into the decision process. This readiness assessment should include the following:

- **Policies and procedures**—New policies and procedures that guide the adoption, management and proper use of cloud computing may be needed.
- **Processes**—Existing processes using traditional IT services may need to be reengineered to incorporate new activities that are related to using cloud services.
- **Organizational structures**—Cloud management may require new organizational capabilities or modifications to existing organizational structures, particularly in IT operations and support.
- **Culture and behavior**—Organizational culture and behavior can be critical for the successful adoption of cloud solutions.
- **Skills and competencies**—Procurement, legal, compliance and audit are some examples of functions that may need to develop necessary skills to manage cloud services from evaluation and sourcing to operations and retirement.

**4. Have management teams considered what existing investments might be lost in their cloud planning?**

Cloud computing may not be an immediate and clean fit with the existing technology portfolio of the enterprise. The adoption of a cloud service may, for example, obviate already-made technology investments that have not reached their planned end date. The decision about when and how to realize that loss must be considered carefully. Areas to consider include:

- **Processes**—The IT organization may need to adapt processes such as sourcing and change management.
- **Culture and behavior**—Cloud services may demand faster turnaround from the IT organization, which may necessitate changes in internal processes and tools.
- **Services, infrastructures and applications**—The enterprise may need to update data centers, software applications and network infrastructures, which may result in some level of lost investment being realized.
- **Skills and competencies**—The IT organization will need to either develop or acquire the skills required to support users of cloud services, if those skills do not already exist within current staffing.

**5. Do management teams have strategies to measure and track the value of cloud return vs. risk?**

Before deciding to adopt cloud computing, the board should give management teams the task of ensuring that proper reporting mechanisms are in place to measure value and risk aligned with enterprise goals.
Conclusion

As cloud services and providers mature, more enterprises will use some form of cloud computing. Boards of directors need to provide guidance to help the enterprise realize the benefits, optimize the risk and control the cost. A good way for boards to initiate this guidance is to ask cloud-specific questions. The answers to these questions can help to determine whether the enterprise is ready to adopt cloud computing and whether the value created will have a positive impact on enterprise goals and objectives.

For a board to know whether cloud services will meet the expectations for cloud computing, it first needs to know whether expectations for cloud computing are aligned to the enterprise strategy. The first step in governing cloud computing is for the board to establish a common understanding of expected benefits and the mechanisms to track and measure them. COBIT 5 and its related products can be used to govern and manage complex investments like cloud services. Using COBIT 5 to implement consistent practices can help to maximize value and control risk.

Understanding the current environment and the relationship between cloud computing and enterprise goals can help to avoid pressure points and optimize risk and resources.

Additional Resources and Feedback
Visit www.isaca.org/cloud-governance 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.