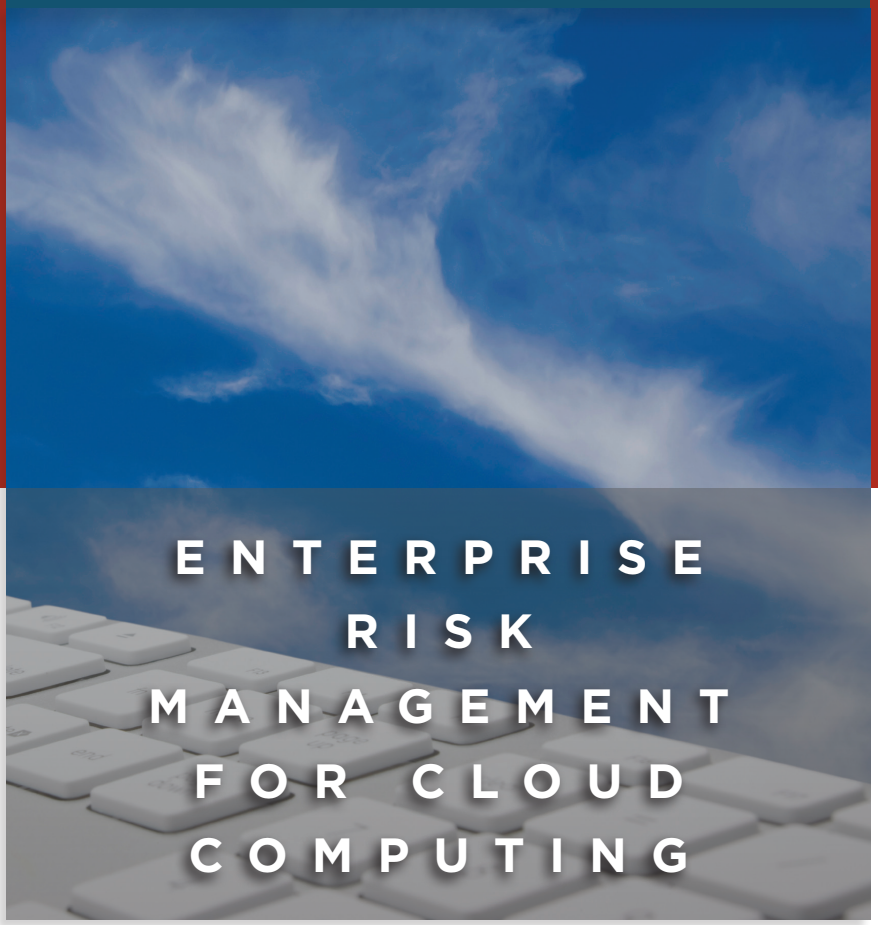
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Thought Leadership in ERM



ENTERPRISE RISK MANAGEMENT FOR CLOUD COMPUTING

By

Crowe Horwath LLP

Warren Chan | Eugene Leung | Heidi Pili

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your professional adviser, and this paper should not be considered substitute for the services of such advisors, nor should it be used as a basis for any decision or action that may affect your organization.

Authors

Crowe Horwath LLP

Principal Contributors

Warren Chan
Principal, IT Risk Services
Crowe Horwath LLP – Chicago
Eugene Leung
IT Risk Services (formerly)
Crowe Horwath LLP – Chicago
Heidi Pili
IT Risk Services (formerly)
Crowe Horwath LLP – Chicago

Quality Assurance

Victoria Cheng
IT Risk Services
Crowe Horwath LLP – Chicago
Larry Rieger
Chief Executive Officer
Crowe Horwath Global Risk Consulting – Chicago

COSO Board Members

David L. Landsittel
COSO Chair

Douglas F. Prawitt
American Accounting Association

Richard F. Chambers
The Institute of Internal Auditors

Marie N. Hollein
Financial Executives International

Chuck E. Landes
American Institute of CPAs (AICPA)

Jeff C. Thomson
Institute of Management Accountants

Sandra Richtermeyer
Institute of Management Accountants

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

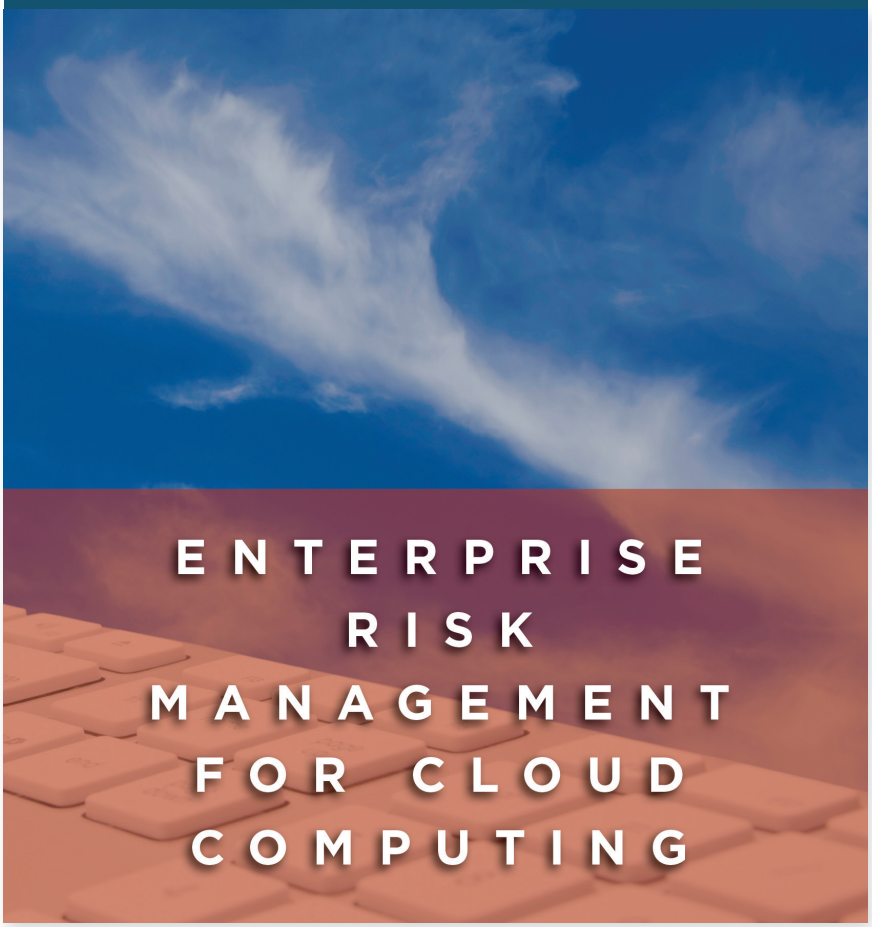
The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

Thought Leadership in ERM



ENTERPRISE RISK MANAGEMENT FOR CLOUD COMPUTING

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

June 2012

Copyright © 2012, The Committee of Sponsoring Organizations of the Treadway Commission (COSO).
1234567890 PIP 198765432

All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted or displayed in any form or by any means without written permission. For information regarding licensing and reprint permissions please contact the American Institute of Certified Public Accountants' licensing and permissions agent for COSO copyrighted materials. Direct all inquiries to copyright@aicpa.org or AICPA, Attn: Manager, Rights and Permissions, 220 Leigh Farm Rd., Durham, NC 27707. Telephone inquiries may be directed to 888-777-7707.

Table of Contents

	Page
COSO Enterprise Risk Management for Cloud Computing	1
1. What Is Cloud Computing?	2
2. The Opportunities	3
3. The Risks	4
4. Changes in the Business Operating Environment with Cloud Computing	6
5. Approaching ERM in the Cloud Computing Paradigm	8
6. Recommended Risk Responses for Cloud Computing	13
7. Cloud Computing Board Oversight, Management Decisions, and Other Considerations	17
8. Conclusion	20
Appendix: Cloud Computing Governance – Roles and Responsibilities	21
About COSO	23
About the Authors	23

COSO Enterprise Risk Management for Cloud Computing

In the evolution of computing technology, information processing has moved from mainframes to personal computers to server-centric computing to the Web. Today, many organizations are seriously considering adopting cloud computing, the next major milestone in technology and business collaboration. A supercharged version of delivering hosted services over the Internet, cloud computing potentially enables organizations to increase their business model capabilities and their ability to meet computing resource demands while avoiding significant investments in infrastructure, training, personnel, and software.

In fall 2010, a Google executive testified before a U.S. congressional subcommittee that more than three million businesses worldwide were customers of its cloud service offerings. Gartner Inc. predicts that cloud computing will be a $140 billion industry by 2014.

Technological advancements in system virtualization, system resource management, and the Internet have led to cloud computing's emergence as a viable alternative for meeting the technology needs of many types of enterprises, with the following benefits resonating with executives:

- Instantaneous computing resource fulfillment;
- Greater value from technology expenditures at lower costs;
- Common technology platforms that can facilitate standardization; and
- Decreased need for internal technology support personnel.

As with any new opportunity, cloud computing entails commensurate risks. It brings to organizations a different dimension of collaboration and human interaction, new organizational dependencies, faster resource fulfillment, and new business models.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management – Integrated Framework* establishes a common language and foundation for organizations to assess and oversee risks from a holistic perspective. Citing a timeless statement made in that publication[1]: "Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value." Cloud computing can present a significant change to the operating environment; use of COSO's *Enterprise Risk Management – Integrated Framework* will facilitate the identification of risks and mitigation strategies with the evolving cloud computing paradigm that presents significant opportunities as well as uncertainty.

The intent of this publication is to leverage the principles of COSO's *Enterprise Risk Management – Integrated Framework* in order to provide guidelines that will identify succinctly the risks and impact cloud computing will have on an organization. The more educated executives become about the risks and benefits of cloud computing, the more effectively they will be able to prepare their organizations for the future. The guidance presented here will enable executives to identify, monitor, and mitigate or accept the risks that come with using cloud computing.

[1] COSO, *Enterprise Risk Management – Integrated Framework*, September 2004, page 3.

1. What Is Cloud Computing?

Definition

Cloud computing is a computing resource deployment and procurement model that enables an organization to obtain its computing resources and applications from any location via an Internet connection. Depending on the cloud solution model an organization adopts, all or parts of the organization's hardware, software, and data might no longer reside on its own technology infrastructure. Instead, all of these resources may reside in a technology center shared with other organizations and managed by a third-party vendor.

Cloud Computing Terminology

- **Cloud service provider (CSP)** – A third-party vendor that provides application delivery, hosting, monitoring, and other services through cloud computing. A single organization can have contractual relationships with multiple CSPs depending on the required cloud solutions.

- **Multi-tenant** – With most CSP technology solutions, a customer is a single tenant among many tenants sharing common resources and technologies. The multi-tenant concept affects how resources are organized and provided to the CSP's customers. For example, a cloud customer's data might be housed in a single large data storage platform that is shared with the data of multiple tenants of the same cloud solution.

Cloud Deployment Models

The most common types of cloud computing deployment models, according to the National Institute of Standards of Technology,[2] are:

- **Private cloud** – The cloud infrastructure is operated solely for an individual organization and managed by the organization or a third party; it can exist on or off the organization's premises.

- **Community cloud** – The cloud infrastructure is shared by several organizations and supports a specific community that has common interests (e.g., mission, industry collaboration, or compliance requirements). It might be managed by the community organizations or a third party and could exist on or off the premises.

- **Public cloud** – The cloud infrastructure is available to the general public or a large industry group and is owned by an organization selling cloud services.

- **Hybrid cloud** – The cloud infrastructure is composed of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Cloud Service Delivery Models

The cloud solutions offered by a CSP usually are referred to as cloud service delivery models, and the most common are:

- **Software as a Service (SaaS)** – Applications organizations use to perform specific functions or processes (e.g., email, customer management systems, enterprise resource planning systems, and spreadsheets). A more evolved offering of SaaS that is gaining popularity at the time of publication is known as Business Process as a Service (BPaaS). With BPaaS, entire business processes (e.g., payroll and supply-chain management) are outsourced to a third-party provider and supported by combinations of cloud service delivery solutions.

- **Platform as a Service (PaaS)** – Development environments for building and deploying applications. The CSP provides its customers with proprietary tools that facilitate the creation of application systems and programs that operate on the CSP's hosted infrastructure.

- **Infrastructure as a Service (IaaS)** – The CSP provides an entire virtual data center of resources (e.g., network, computing resources, and storage resources).

[2] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, Special Publication 800-145, http://csrc.nist.gov/publications/PubsSPs.html#800-145.

2. The Opportunities

Some of the opportunities and potential benefits that apply to almost all forms of cloud computing include:

- **Cost savings** – Cloud customers pay for only the computing resources they use rather than purchasing or leasing equipment that may not be fully utilized at all times. If cloud computing is used to meet all the technology needs of an organization, there are no longer physical space requirements and utility costs traditionally associated with maintaining a dedicated data center environment. An organization that obtains all of its computing resources from a cloud service provider can expense all the dollars (i.e., receive a U.S. tax benefit). This tax benefit does not typically apply to internal dedicated data centers in which capital expenditures and amortization factors are involved.

- **Speed of deployment** – Cloud service providers can meet the need for computing resources (e.g., server processing and data storage) much more quickly than most internal information technology (IT) functions. The time to fulfill requests for computing power and applications can change from months to weeks, weeks to days, and days to hours.

- **Scalability and better alignment of technology resources** – An organization can scale up and down its capacity from one server to hundreds of servers without capital expenditures. This ability enables an organization to obtain large amounts of computing resources for performing temporary computing-intensive tasks when needed without investing in excess computing capacity to meet infrequent high-demand periods.

- **Decreased effort in managing technology** – Owning and operating an IT function is costly and time-consuming. Cloud computing allows an organization to focus more time on its core purpose and goals. Most cloud service offerings are based on a prebuilt standardized foundation of technology that facilitates better support. This foundation also makes provisioning computing resources easier, which in turn paves the way for more consistent technology upgrades and expedited fulfillment of IT resource requests.

- **Environmental benefits** – If every organization were to replace its private data center with cloud computing, the result would be significantly less overall power consumption, carbon emissions, and physical land use.

3. The Risks

As defined in COSO's 2004 *Enterprise Risk Management – Integrated Framework*[3]: "Risk is the possibility that an event will occur and adversely affect the achievement of objectives."

The types of risks (e.g., security, integrity, availability, and performance) are the same with systems in the cloud as they are with non-cloud technology solutions. An organization's level of risk and risk profile will in most cases change if cloud solutions are adopted (depending on how and for what purpose the cloud solutions are used). This is due to the increase or decrease in likelihood and impact with respect to the risk events (inherent and residual) associated with the CSP that has been engaged for services.

Some of the typical risks associated with cloud computing are:

- **Disruptive force** – Facilitating innovation (with increased speed) and the cost-savings aspects of cloud computing can themselves be viewed as risk events for some organizations. By lowering the barriers of entry for new competitors, cloud computing could threaten or disrupt some business models, even rendering them obsolete in the future. For example, streaming media over the Internet was a technology solution that significantly reduced the sales of CDs and DVDs and the need for physical retail stores. Existing competitors that fully embrace the cloud might be able to bring new ideas and innovation into their markets faster. Since cloud computing solutions yield considerable short-term cost savings due to reduced capital expenditures, an organization adopting the cloud might be able to extract better margins than its non-cloud competitors. Thus, when an industry member adopts cloud solutions, other organizations in the industry could be forced to follow suit and adopt cloud computing.

- **Residing in the same risk ecosystem as the CSP and other tenants of the cloud** – When an organization adopts third-party-managed cloud solutions, new dependency relationships with the CSP are created with respect to legal liability, the risk universe, incident escalation, incident response, and other areas. The actions of the CSP and fellow cloud tenants can impact the organization in various ways. Consider the following:

  - Legally, third-party cloud service providers and their customer organizations are distinct enterprises. However, if the CSP neglects or fails in its responsibilities, it could have legal liability implications for the CSP's customer organizations. But if a cloud customer organization fails in its responsibilities, it is less likely there would be any legal implications to the CSP.

  - Cloud service providers and their customer organizations are likely to have separate enterprise risk management (ERM) programs to address their respective universe of perceived risks. Only in a minority of cases (involving very high-dollar contracts) will CSPs attempt to integrate portions of their ERM programs with those of their customers. The universe of risks confronting an organization using third-party cloud computing is a combination of risks the individual organization faces along with a subset of the risks that its CSP is facing (discussed further in Section 5, "Approaching ERM in the Cloud Computing Paradigm").

- **Lack of transparency** – A CSP is unlikely to divulge detailed information about its processes, operations, controls, and methodologies. For instance, cloud customers have little insight into the storage location(s) of data, algorithms used by the CSP to provision or allocate computing resources, the specific controls used to secure components of the cloud computing architecture, or how customer data is segregated within the cloud.

- **Reliability and performance issues** – System failure is a risk event that can occur in any computing environment but poses unique challenges with cloud computing. Although service-level agreements can be structured to meet particular requirements, CSP solutions might sometimes be unable to meet these performance metrics if a cloud tenant or incident puts an unexpected resource demand on the cloud infrastructure.

- **Vendor lock-in and lack of application portability or interoperability** – Many CSPs offer application software development tools with their cloud solutions. When these tools are proprietary, they may create applications that work only within the CSP's specific solution architecture. Consequently, these new applications (created by these proprietary tools) might not work well with systems residing outside of the cloud solution. In addition, the more applications developed with these proprietary tools and the more organizational data stored in a specific CSP's cloud solution, the more difficult it becomes to change providers.

[3] COSO, *Enterprise Risk Management – Integrated Framework*, September 2004, page 16.

- **Security and compliance concerns** – Depending on the processes cloud computing is supporting, security and retention issues can arise with respect to complying with regulations and laws such as the *Sarbanes-Oxley Act of 2002* (SOX), the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), and the various data privacy and protection regulations enacted in different countries. Examples of these data privacy and protection laws would include the *USA PATRIOT Act*, the EU Data Protection Directive, Malaysia's *Personal Data Protection Act 2010*, and India's *IT Amendments Act*. In the cloud, data is located on hardware outside of the organization's direct control. Depending on the cloud solution used (SaaS, PaaS, or IaaS), a cloud customer organization may be unable to obtain and review network operations or security incident logs because they are in the possession of the CSP. The CSP may be under no obligation to reveal this information or might be unable to do so without violating the confidentiality of the other tenants sharing the cloud infrastructure.

- **High-value cyber-attack targets** – The consolidation of multiple organizations operating on a CSP's infrastructure presents a more attractive target than a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a CSP solution in most cases are higher with respect to confidentiality and data integrity.

- **Risk of data leakage** – A multi-tenant cloud environment in which user organizations and applications share resources presents a risk of data leakage that does not exist when dedicated servers and resources are used exclusively by one organization. This risk of data leakage presents an additional point of consideration with respect to meeting data privacy and confidentiality requirements.

- **IT organizational changes** – If cloud computing is adopted to a significant degree, an organization needs fewer internal IT personnel in the areas of infrastructure management, technology deployment, application development, and maintenance. The morale and dedication of remaining IT staff members could be at risk as a result.

- **Cloud service provider viability** – Many cloud service providers are relatively young companies, or the cloud computing business line is a new one for a well-established company. Hence the projected longevity and profitability of cloud services are unknown. At the time of publication, some CSPs are curtailing their cloud service offerings because they are not profitable. Cloud computing service providers might eventually go through a consolidation period. As a result, CSP customers might face operational disruptions or incur the time and expense of researching and adopting an alternative solution, such as converting back to in-house hosted solutions.

In addition to these risks, certain characteristics of cloud computing may give rise to other less apparent challenges that warrant evaluation (these less apparent points are discussed in the "Other Considerations" portion of Section 7 of this document).

Some management teams may be willing to accept the risks of running their entire enterprise in a public cloud given the small up-front capital investment requirements. Start-ups and venture capitalists are likely to prefer focusing their investments on the business model rather than a technology infrastructure that would be of limited value if the venture were to fail. Start-ups can deploy their business models supported by cloud solutions more quickly and more economically in comparison to the previous generation of technology options.

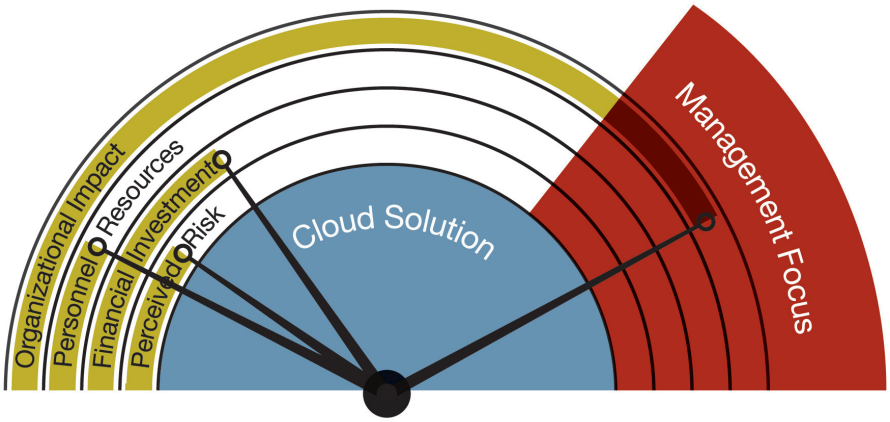
All of the cloud computing risks discussed here should be given careful consideration (that is, undergo a risk assessment), as the materialization of any of these risks will present very undesirable consequences. Many of the risks highlighted here are not likely to be mitigated by contractual clauses with a CSP (assuming the contract is even negotiable – most commodity cloud contracts are not). Consequently, mitigation solutions may need to be implemented outside of the immediate cloud solution provided by the CSP.

4. Changes in the Business Operating Environment with Cloud Computing

An organization should recognize the risks and other effects cloud computing can have on its operating environment and account for them in its ERM programs. In some cases, cloud computing can easily enter into an organization while bypassing typical management oversight controls. When an organization invests significant resources in an endeavor that could take months or years to complete, conventional processes and controls require management's involvement and approval. Such endeavors are highly likely to attract senior management's attention in the form of risk assessments, audits, and steering committees.

Some cloud solutions can easily be adopted within a short period of time while requiring a small monetary investment and the involvement of very few personnel. The equation of big investment equals big impact is different with cloud computing, where a small investment can have a big impact. The need to expend a great amount of effort to analyze cloud computing risks and perform the related due diligence may be counterintuitive. Consequently, management could neglect to perform time-consuming steps such as confirming compliance with legal or regulatory requirements or evaluating the potential impact of the CSP on the organization's operations and risk profile. **Exhibit 4.1** illustrates how with cloud computing, some of the typical control trigger points (such as personnel resources and required finances) might not reach the levels that would typically invoke the oversight of senior management.

Exhibit 4.1 Cloud Solutions Can Be Adopted While Eluding Management Oversight

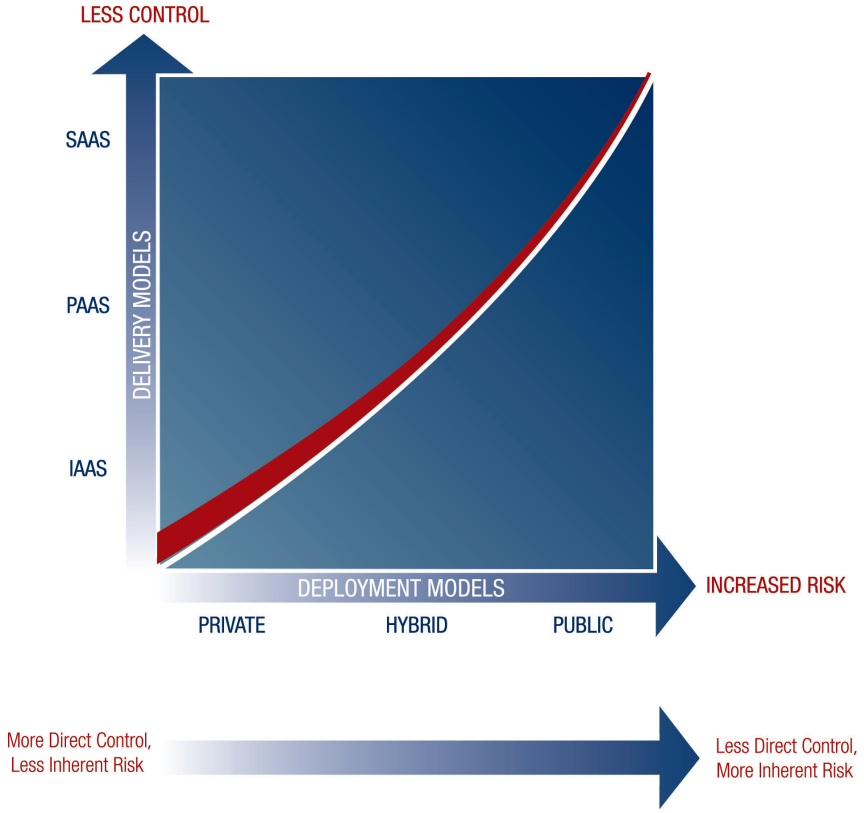


It is paramount that management also understands that with most cloud solutions (with the possible exception of an internal private cloud) the organization has less direct control of the solution and consequently a higher level of inherent risk.

For example, an organization using a SaaS (public cloud) solution has shifted responsibility for some or all of its IT functions, including controls, to a third-party provider. **Exhibit 4.2** illustrates the degree of control the organization retains and relinquishes, depending on the type of cloud service delivery and the deployment model.

Specifically, the maximum amount of control and least amount of inherent risk are associated with an IaaS (private cloud) solution. In contrast, with a SaaS (public cloud) solution, the organization retains the least amount of control and must accept the highest level of inherent risk. In all cases, management should evaluate the cloud deployment and delivery models in the context of acceptable risk levels as this will determine the preferred type of cloud computing environment and related requisite controls.

Exhibit 4.2 Inherent Risk Relationship with Cloud Service Delivery and Deployment Models



5. Approaching ERM in the Cloud Computing Paradigm

The advent of cloud computing should be considered an event in the operating environment of an organization's ERM program.

As with any endeavor, defining objectives and courses of actions in advance increases the chances of success. Consequently, a well-developed plan that clearly defines the organization's objectives and the specifics of cloud computing's role will enable management to make sound decisions. Some of the ERM prerequisites that should be factored into a quality cloud computing plan, and ultimately the cloud solution, are a strong governance model, a sound reporting structure, an accurate understanding of internal IT skills and abilities, and a defined risk appetite.

Some management teams view risk assessments and governance programs as optional. It is not uncommon for organizations to adopt cloud computing solutions without applying a formal risk evaluation or expending any effort to adjust its ERM or governance program. It is a best practice to incorporate cloud governance in the initial stages (when a cloud computing strategy is being defined) before a cloud solution is adopted. For organizations that already have adopted cloud computing without following best ERM practices, it is still prudent to perform a risk assessment and establish cloud governance.

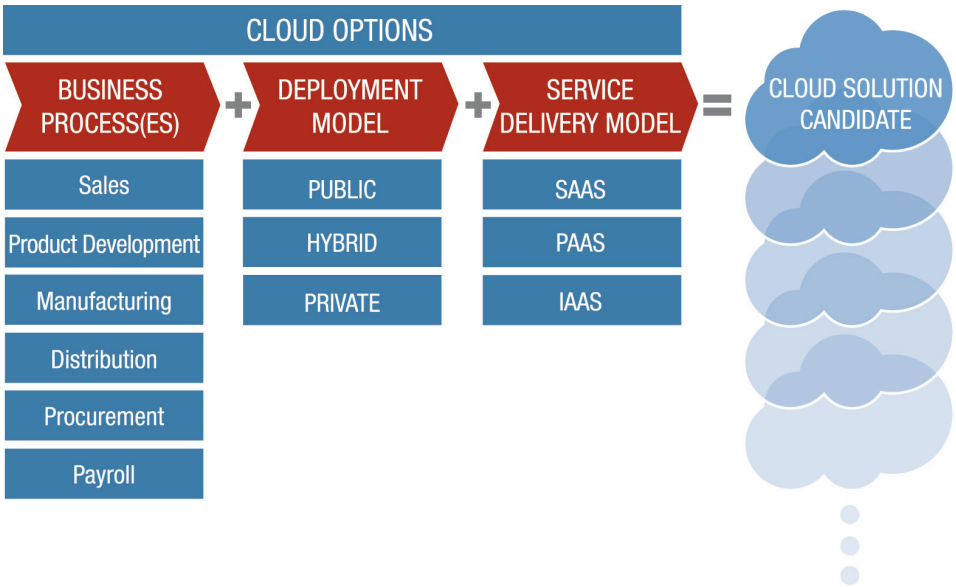
Establishing Cloud Computing Governance Using the COSO Framework

The degree of adjustment required to an organization's existing ERM program in a cloud computing paradigm depends greatly on the business processes the cloud supports, the deployment model, the service delivery model, and the nature of the engaged CSP's risks and control environment.

In many cloud scenarios, the organization no longer has complete or direct control over technology and technology-related management processes. Management must determine if it has the risk appetite for the entire universe of potential events associated with a given cloud solution as some of these events extend beyond the organization's traditional borders and include some events that have an impact on the CSP (or CSPs) supporting the organization.

Exhibit 5.1 depicts how specific cloud solution candidates are derived by choosing among the various options with respect to cloud-supported business processes, deployment models, and service delivery models.

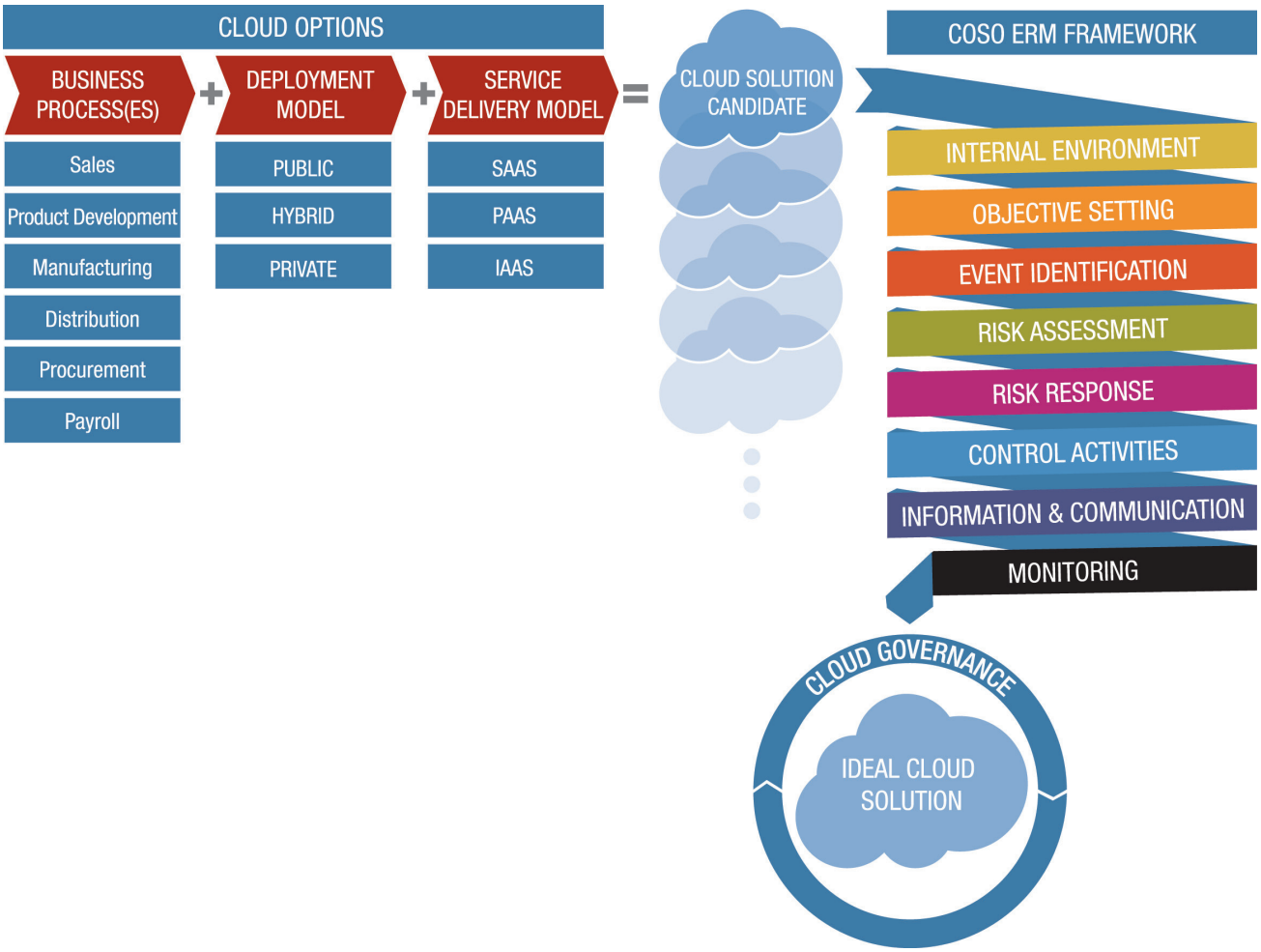
Exhibit 5.1 Cloud Solution Creation



While adopting cloud computing could be a major change for an organization, management can use a proven ERM framework to effectively assess and manage the related risks. The framework put forth in COSO's *Enterprise Risk Management – Integrated Framework* has established a common language and foundation that can be used to construct an effective cloud governance program tailored specifically for a given cloud solution.

The original COSO ERM framework was illustrated as a cube. In **Exhibit 5.2**, the framework is represented as a pathway in which each ERM component (starting with internal environment) is applied in order to understand the specific advantages and disadvantages that a given solution candidate would bring to the organization. When the process is completed for each cloud solution candidate, the ideal cloud solution will emerge along with its related requisites for establishing cloud governance.

Exhibit 5.2 Applying the COSO ERM Framework to Cloud Computing Options



In cases where a cloud solution has already been implemented, the COSO ERM framework can be used to establish, refine, or perform a quality assurance check of the cloud governance program by ensuring that all major aspects of the program (e.g., objectives, risk assessment, and risk response) have been addressed with respect to management's requirements. An effective cloud governance program can still be achieved by applying the COSO ERM framework after the implementation of a cloud solution.

The best-practice situation is when management uses the COSO ERM framework to identify the ideal configuration of cloud solution options (i.e., business process, deployment model, and service delivery model) that fits management's risk appetite. By evaluating the cloud solution candidates in the context of each component of the COSO ERM framework, management can succinctly identify the related risks and desired risk acceptance or mitigation strategies with each cloud solution scenario (as risks will vary with each combination of options). This evaluation will enable management to make prudent risk management and governance decisions in selecting its ideal set of cloud solution options and creating a well-thought-out cloud governance program before the cloud solution is implemented.

The remaining material of this section elaborates on some of the key concepts with respect to evaluating cloud solution candidates through each of the components of the COSO ERM framework:

Internal Environment – The internal environment component serves as the foundation for and defines the organization's risk appetite in terms of how risks and controls are viewed. For instance, if management has a policy of not outsourcing any of its operations (i.e., there is a culture of risk avoidance), this policy will limit the viable options for cloud deployment and service delivery models so that private cloud solutions might be the only acceptable alternative.

Objective Setting – Management needs to evaluate how cloud computing aligns with the organization's objectives. Depending on the circumstances, cloud computing might present an opportunity for the organization to enhance its ability to achieve existing objectives, or it might present an opportunity to gain a competitive advantage, which would require new objectives to be defined.

Event Identification – Management is responsible for identifying the events (either opportunities or risks) that can affect the achievement of objectives. The complexity of event identification and risk assessment processes increases when an organization engages cloud service providers.

Management needs to consider external environmental factors (e.g., regulatory, economic, natural, political, social, and technological), as well as the organization's internal factors (e.g., culture, personnel, and financial health), as part of the process when identifying and assessing risk events. With the use of public or hybrid cloud solutions, management needs to take into consideration events affected by external and internal factors of its CSP as well. Management should endeavor to have a complete inventory of events, since the nature and quality of the risk assessment process is significantly influenced by the expected events.

Risk Assessment – Management should evaluate the risk events associated with its cloud strategy to determine the potential impact of the risks associated with each cloud computing option. Ideally, risk assessments should be completed before an organization moves to a cloud solution.

Cloud computing can affect the following critical focal points of a risk assessment:

- **Risk profile** – An organization's risk profile encompasses the entire population of risks it must manage. When a cloud solution is adopted, an organization's risk profile is altered due to changes in the likelihood of risks, the potential impact of the risks, and the inclusion of a subset of the CSP's risk universe (refer to "Risk Profile Impact of CSPs and Fellow Cloud Tenants" discussion at the end of this section).

- **Inherent and residual risk** – An organization must assess the inherent risks of the events and then develop risk responses and determine the residual risk. Depending on the organization, the non-cloud computing solutions' inherent and residual risk levels could be either greater or less than those of the cloud computing options.

- **Likelihood and impact** – The likelihood of certain events and the related potential impact change in many cases when cloud solutions are adopted. The ability to make this determination accurately depends on whether the organization has a comprehensive, accurate, and current inventory of risks.

In some situations, management will not have access to all the required information related to the CSP's internal control environment; consequently, certain assumptions will have to be made in order to complete the risk assessment.

Risk Response – Once risks have been identified and assessed in the context of organizational objectives relative to cloud computing, management needs to determine its risk response. There are four types of risk responses:

- **Avoidance** – Exiting the activities giving rise to risk (i.e., not moving to the cloud or considering only private cloud types of solutions as viable options).
- **Reduction** – Implementing control activities and taking actions to reduce risk likelihood, risk impact, or both.
- **Sharing** – Reducing risk likelihood or risk impact by transferring or otherwise sharing a portion of the risk (e.g., buying insurance).
- **Acceptance** – Taking no action to affect risk likelihood or impact. For example, when an organization does not have direct ability to manage the controls of its CSP, the organization is accepting an increased level of inherent risk.

With most hybrid or public cloud solutions, management relies on third-party-managed controls; this reduces management's ability to mitigate the risks directly. This implies that the levels of inherent risk will be increased with the adoption of most CSP solutions, and as a result management will likely need to increase its risk appetite.

Due to the significant role that risk response plays in cloud computing, an expanded discussion is presented in Section 6, "Recommended Risk Responses for Cloud Computing."

Control Activities – The traditional types of controls – preventive, detective, manual, automated, and entity-level – apply to cloud computing as well. The difference introduced by cloud computing is that some control responsibilities might remain with the organization while certain control responsibilities will be transferred to the CSP.

If the quality of an organization's existing control activities is moderate or poor, going to a cloud solution could exacerbate internal control weaknesses. For example, if an organization with poor password controls or data security practices migrates its computing environment to a public or hybrid cloud solution, the possibility of an external security breach is likely to increase significantly due to the fact that access to the organization's technology base is now through the public Internet.

Information and Communication – To effectively operate its business and manage the related risks, management relies on timely and accurate information and communications from various sources regarding external and internal events. With cloud computing, information received from a CSP might not be as timely or of the same quality as information from an internal IT function. As a result, fulfilling management's information and communications requirements might require additional or different information processes and sources.

Management should also monitor external information related to its CSP (e.g., financial reports, public disclosures, regulatory filings, industry periodicals, and announcements by fellow cloud tenants), since certain events impacting the CSP or fellow cloud tenants might also have an impact on the organization.

Monitoring – "Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or entity objectives may change." That statement from 2004 in the COSO's *Enterprise Risk Management – Integrated Framework*[4] remains applicable in the age of cloud computing. Management must continue to monitor the effectiveness of its ERM program to verify that the program adequately addresses the relevant risks and facilitates achieving the organization's objectives. Effective ERM programs are evolving and dynamic in nature and must be increasingly so given the pace of cloud computing's evolution in terms of solution offerings, competitors' adopting the cloud, and changing laws.

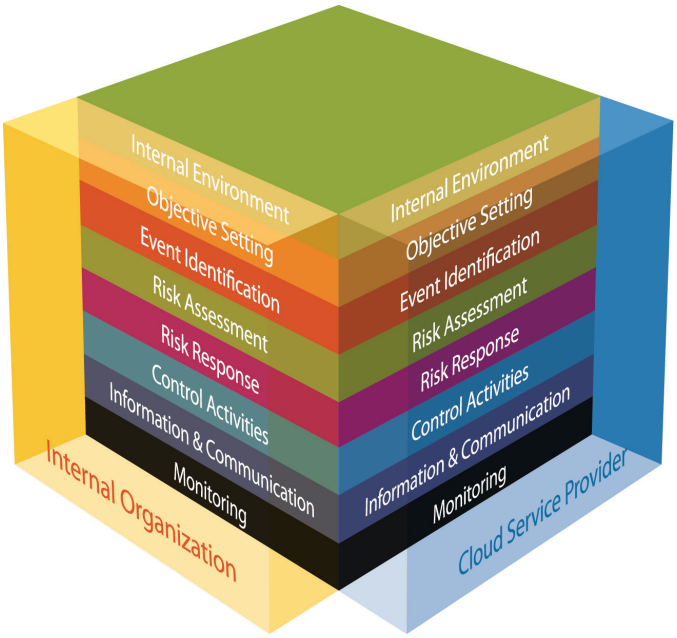
Given cloud computing's potential and actual impact, senior management personnel across the enterprise (not limited to the chief information officer) need to be assigned responsibilities to achieve cloud computing governance. ("Appendix: Cloud Computing Governance – Roles and Responsibilities" provides examples of the assignment of some of these key cloud computing responsibilities.)

[4] COSO, *Enterprise Risk Management – Integrated Framework*, September 2004, page 75.

Risk Profile Impact of CSPs and Fellow Cloud Tenants

An organization moving from a dedicated internal computing environment to a public or hybrid cloud computing solution ultimately is converting its organization's ERM component universe into a combination of its own ERM component universe and the ERM component universe of its contracted CSP. **Exhibit 5.3** depicts this concept.

Exhibit 5.3 Combined ERM Component Universe of an Organization with Its CSP



The organization's data and processes are hosted in a shared environment with other cloud tenants. The behavior and events of the CSP and fellow tenants could have a direct impact on the organization. Since the risks to which a CSP is exposed can have an impact on its cloud customers, these risks must be incorporated into the risk profile of all the organizations using the CSP's solutions. This blending of environments is likely to change the organization's risk profile and therefore require new and different controls. This combining of risk profiles might also extend to fellow tenants that are sharing the same cloud infrastructure resources.

As part of its cloud risk assessment process, management may need to consider risk-related information about its fellow tenants – for example, their identities, the applications they deploy, and their likelihood of becoming targets of cyber-attacks.

Consequently, management's ERM program should address the combined universe of its own organization's ERM components along with the ERM components of the CSP. Management needs to identify the risks and events that could affect its own organization and those that could affect its CSP and fellow cloud tenants.

6. Recommended Risk Responses for Cloud Computing

With the advent of cloud computing, every organization is operating in an environment that is rapidly changing, irrespective of management's opinions or decisions about joining cloud computing. Management should adapt the organization's ERM programs and controls accordingly. The following section elaborates on recommended risk responses for some of the more significant cloud-related risks presented in this publication.

Risk – Unauthorized cloud activity

Risk Response – Cloud policies and controls

All organizations should have policies to establish controls to prevent and detect the unauthorized procurement and use of cloud services, regardless of management's position on venturing into cloud computing. Due to the low cost of initiating cloud services relative to traditional technology purchases, current controls such as expenditure limits may not trigger appropriate attention from management.

> For example, a small business unit of a large corporation independently decided to leverage a cloud-based customer relationship management (CRM) system for a new product's sales initiative. With no established corporate cloud policy, the business unit started this initiative without engaging the internal IT group or making a capital expenditure request. (The cloud solution required only Internet access and a credit card.) Once launched, the system was populated with data about customers and prospects. Consequently, confidential customer information was being stored outside the corporation's internal computing environment without being subject to the organization's controls or operating procedures.

For organizations that have decided to adopt cloud computing, the following are some suggested risk responses with respect to unauthorized cloud activity:

- Establish a cloud usage policy that clearly articulates the business processes and data that management deems appropriate to be supported by cloud computing solutions;
- Create or update a policy that identifies who is authorized to procure cloud computing services;
- Identify approved cloud vendors; and
- Define policy and communicate guidance on the management of relationships with CSPs.

Risk – Lack of transparency

Response – Assessments of the CSP control environment

Completing a high-quality and thorough risk assessment of a CSP environment can be challenging when the desired information is incomplete or difficult to obtain. In most cases, a CSP's internal control environment is not completely visible to its customers.

For example, change management controls such as user acceptance testing and segregation of production and development environments are normally used to ensure the quality of applications systems. With a public or hybrid SaaS cloud solution, cloud customer organizations do not have direct control or detailed knowledge of the CSP's application change management controls. Consequently, the cloud customers of the SaaS solution may need to augment or change their processes for testing application changes, depending on their risk appetites and what the CSP discloses in its Service Organization Control (SOC) Reports (assuming the CSP has incurred the expense of creating SOC Reports).

To partially overcome the challenges of gaining insight into a CSP's operations and controls, management should include control-related inquiries in a request for proposal or in the due diligence process. Management should also attempt to include a right-to-audit clause in the contract with each CSP. As part of assessing the CSP's internal environment, management should (preferably before the CSP is engaged) conduct interviews to determine how the CSP would address certain risk events. For further knowledge about the risks and quality of the CSP's internal control environment and cloud solutions, management could have its internal audit function perform an evaluation, or management could require the CSP to provide independent audit reports such as those defined by the American Institute of Certified Public Accountants (AICPA) with respect to the Statement on Standards for Attestation Engagements 16 (SSAE16) and the Service Organization Control 2 (SOC 2) reports including areas of security, availability, processing integrity, confidentiality, or privacy.

Risks – Security, compliance, data leakage, and data jurisdiction

Response – Data classification policies and processes

Moving to public or hybrid cloud computing solutions could change current locations of data storage, transaction processing, and control structures. These changes require analysis since they are likely to have an impact on how the organization's operations remain compliant with applicable laws and regulations. Contractual language should clearly define the CSP's responsibilities regarding meeting compliance and regulatory requirements on behalf of the organization.

If an organization's data resides in a cloud solution (with the possible exception of a private cloud), there is no ability to identify the data's specific current location (server or storage device) or the data's residence history of locations. (Note that a few CSPs do offer an option to specify the desired country of residence for data in their possession.) This location challenge is due to the nature of multi-tenant cloud environments in which resources are reused and dynamically allocated to cloud customers. This inability to identify the specific locations of data storage and processing with cloud solutions may present obstacles in meeting e-discovery or data lineage requirements. This limitation could have a big impact on the data storage or (to a lesser extent) transaction processing activities that an organization might want to have supported by cloud computing.

CSP contract terms related to country location (i.e., domestic or international) of customer data should be determined and evaluated with respect to data protection law compliance. Some commodity CSPs may not reveal their locations but may share some information regarding the jurisdictions with which they must legally comply. It is a prudent precautionary action for management to understand the regulatory implications and legal jurisdiction responsibilities with respect to its organization's data in advance of moving to a third-party hosted cloud solution. Take, for example, a U.S.-based CSP that controls data in Germany. This CSP must comply with German data protection laws and EU data protection and notification laws and is also subject to the *USA PATRIOT Act* requirements. Compliance and data jurisdiction are not new concepts to organizations; however, engaging in the cloud heightens the need to review approaches in terms of obligations in these areas.

While an organization cannot control exactly where its data is stored when using a public or hybrid cloud deployment model, it can control the type of information that resides in the cloud. From a risk management perspective, it is critical for any organization using public or hybrid cloud computing solutions to have effective data classification policies and processes in place.

Data classification policies should clearly define the types of information deemed sensitive and prohibited from residing outside of the organization's direct control. Ultimately, data classification policies should ensure that the purpose, ownership, and sensitivity of different types of organizational data are clearly communicated and understood throughout the organization.

These policies should be supported by data classification processes that include the following:

- Mapping legal, regulatory, intellectual property, and security requirements to the various types of data;
- Determining the sensitivity (public, restricted, or highly sensitive) of the various types of data;
- Establishing requirements (such as encryption) for data transmission; and
- Identifying data owners – individuals who have the proper knowledge and authority to decide who should be granted data access and the type of data access (e.g., a business manager or compliance officer).

Risks – Transparency and relinquishing direct control

Response – Management oversight and operations monitoring controls

In non-outsourcing situations, management can take direct action regarding all facets of its internal control environment. In the public or hybrid cloud models, management transfers partial or complete direct control to the CSP. In most situations, the CSP is focused on providing a stable and secure platform that meets the control requirements of its customers from a macro perspective. The CSP's solutions are not likely to satisfy every unique need of every cloud customer. It is the responsibility of management to assess the CSP's cloud solution in detail and implement additional controls so that the CSP's cloud solution meets all of the organization's requirements.

Management needs to have a precise understanding of the controls it is relinquishing to its CSP as this understanding will determine the specific monitoring controls that management should implement. In the case of a publicly held company, added precautions should be applied if management is relinquishing those controls that affect management's financial statement assertions. Migrating to cloud computing does not mean management can be worry free.

Maintaining the control environment of the organization's cloud solution might be a joint responsibility of management and the CSP it engages. Third-party audit reports of a CSP (such as SOC reports) include a complementary user entity controls component that defines the responsibilities of the customers of the CSP's services, thus explicitly excluding these duties from the CSP's control responsibilities. Consequently, management must be sure to incorporate the complementary user entity controls into the organization's control environment. In some situations, there is added complexity in those cases where the contracted CSP has subcontracted (i.e., carve-outs) some of its responsibilities to another provider. If this is the case, SOC reports from all applicable CSPs should be obtained in order to have a complete understanding of outsourced controls. Optimally, to prevent this type of complex situation from materializing, the CSP contract should preclude any form of subcontracting.

An organization using hybrid or public cloud computing solutions should validate the control activities of its CSP to ensure that they align with management's risk appetite. The organization should also periodically verify the effectiveness of the controls maintained by the CSP. Depending on the selected cloud service delivery model, control responsibility between the organization and its CSP might be shared in the areas of implementation, technology operations, and user access administration.

Risks – Reliability, performance, high-value cyber-attack target

Response – Incident management

An organization needs to evaluate its CSP's capability to provide adequate incident response in addition to its own incident response procedures for system disruption and data theft scenarios.

A CSP's system failure or security breach is likely to affect multiple customers. When these types of events occur, the CSP's initial focus will be to resolve the issue for its cloud environment; that is, the CSP is unlikely to focus on addressing the issues of each tenant individually. As a result, management's incident response plan should not rely solely on its CSP unless management is willing to accept the worst-case scenario for CSP support if an adverse incident were to occur.

The following examples elaborate on the inherent risks and related mitigation controls for situations related to cloud solution system failure (i.e., reliability) and cyber-attacks:

System Failure – System failure is a risk event that can occur in any computing environment. In the event of a catastrophic system failure and multiple tenants simultaneously requiring support, lower-priority organizations might not receive the required service level response from the CSP.

Controls that can mitigate the risk of system failure

- Engage other CSPs that have the same solution as your primary CSP and maintain copies of your organization's data so it can easily be deployed to the backup CSP;
- Implement processes to monitor system availability;
- Implement automated tools that provide resources on demand for the cloud solution from another service provider; and
- Review service-level agreements to ensure that the CSP will provide adequate response in the event of system failures.

Cyber-attacks – Every organization has an inherent risk of cyber-attacks on its systems. The consolidation of multiple large organizations on a CSP's infrastructure presents to hackers a larger and possibly a more well-known target. Consider a situation in which a small and obscure company is sharing the cloud infrastructure of a high-profile organization or CSP; the small company's likelihood of being a target of a cyber-attack escalates to the same level as that of the well-known organization or high-profile CSP.

Controls that can mitigate the risk of cyber-attacks

- Host only nonessential and nonsensitive data on third-party CSP solutions;
- Deploy encryption over data hosted on cloud solutions; and
- Have a defined fail-over strategy that would leverage another CSP's solution or an internal solution.

A less obvious situation warranting incident response is the possibility that an organization using public cloud solutions is exposing its operations to the public eye or news coverage if an adverse event were to occur. For example, if a well-known CSP (e.g., Amazon or Google) were to experience a service disruption or security breach from a cyber-attack, the incident likely would garner significant, immediate publicity. The CSP might not have on-hand answers about the affected cloud customer organizations, cause of the problem, estimated time to recovery, or the incident's impact. However, the reputation of any organization known to be a customer of the affected CSP could be damaged even if its operations were unaffected by the incident.

Risk – Noncompliance with regulations

Response – Monitoring of the external environment

Management needs to monitor for changes in the external environment that would affect its own operations and the operations of its CSP. Changes to regulations or telecommunication providers may have a significant impact on how cloud computing can be used.

Major regulatory changes are anticipated in the area of data privacy. Various countries are implementing protective measures to restrict moving and storing their citizens' personally identifiable information outside of their country borders. As a result, cloud-based solutions may need to be designed to store certain data within specific countries' borders instead of storing the data in a country that is at the CSP's discretion.

Risk – Vendor lock-in

Response – Preparation of an exit strategy

The more an organization uses a CSP's solution and the longer it uses the solution to support its operations, the more it depends on the CSP. Nothing lasts forever; it would be prudent for management to anticipate the future need for changing CSP vendors or moving off a cloud solution. Consequently, management should develop an exit strategy or contingency plan as part of its overall cloud strategy.

Risk – Noncompliance with disclosure requirements

Response – New disclosures in financial reporting

New disclosures may be required of publicly traded companies that rely on CSPs to support their critical business processes. In light of cloud computing solutions' potential impact on business operations and other risk factors, public companies need to remain aware of the disclosures they are required to make as part of their regulatory compliance and transparency obligations.

7. Cloud Computing Board Oversight, Management Decisions, and Other Considerations

Cloud Computing Board Oversight

Given the opportunities cloud computing affords and the potential magnitude of its risk impact, cloud computing should be considered in the organization's overall governance activities and regarded as a topic warranting discussion and inquiry by an organization's board.

The following is a list of questions an organization's board of directors should consider posing in its governance oversight role:

- What level of consideration has management given to adopting cloud computing, and what is management's current position on this area?
- Who in management is responsible for understanding and managing the business risks associated with cloud computing?
- What are competitors doing with cloud solutions?
- Does management have effective processes in place to monitor cloud computing adoption and usage?
- What would be the impact of cloud computing to management's overall internal control structure (improved, unchanged, or diminished)?
- Does management have the skills required to understand the complexities associated with cloud computing?
- Are cloud computing initiatives aligned with the organization's risk appetite?
- Are due diligence processes adequate for addressing cloud computing vendors at both the initial contract stage and the engaged stage (which requires monitoring processes)?
- Has management established adequate minimum service-level expectations for third-party cloud providers?
- How is management mitigating organizational risks resulting from reliance on the activities of a third-party cloud service provider?
- If cloud computing solutions are being used to support the organization, have cloud computing risks been determined and disclosed to investors (where applicable)?

Cloud Computing Management Decisions

Deciding whether to adopt cloud computing requires management to evaluate the internal environment – including the state of business operations, process standardization, IT costs, and the backlog of IT projects – along with the external environment – which includes laws and regulations and the competition's adoption of cloud computing.

As management contemplates its cloud computing position and strategies, it should address some key questions, including:

- What is management's stance on outsourcing functions?
- Does the organization anticipate rapid growth that might require using cloud solutions?
- Is the organization in a mature market that might require using cloud computing to save costs to remain competitive?
- Are the organization's operational functions and processes mature and formalized enough to allow for a change in the underlying technology platform?
- What is the capability and maturity of the organization's current IT function?
- How should the organization prepare for cloud computing?
- Should cloud computing be embraced, to capitalize on its benefits, or rejected, to avoid risks such as data breaches or noncompliance with complex e-discovery requirements?
- Who should be involved in the evaluation process, and who makes the decisions?
- How can the organization manage its risks adequately while operating in a business environment with cloud computing?

The variables to be considered when making decisions about cloud computing solutions include business processes to be supported, specific deployment models, specific service delivery models, and the specific vendors that could become service providers.

It should be noted that at publication time, many cloud service providers' offerings are commoditized solutions sold with one-size-fits-all contracts and service-level agreements that are take it or leave it, rather than have it your way.

As with other business decisions, performing a return on investment analysis, total cost of ownership analysis, and prospective vendor due diligence – plus starting with a pilot program – are prudent courses of action.

Other Considerations

The following are some additional and less apparent aspects that deserve serious consideration when making any cloud decisions (as they may give rise to incremental or new risks):

- **Cloud solution pricing predictability** – Many CSPs offer a pay-as-you-go pricing model, which makes calculating the cost of the cloud services appear simple. However, the ability to determine the return on investment a few years down the road is encumbered by cloud computing's limited existing price trending history on which to base calculations. For example, can management predict whether the prices of cloud solutions will rise or fall in the future? How long will the current pricing of cloud services remain in effect? Are caps on pricing increases stipulated in contracts?

- **Captive renter** – The longer an organization is a partner with a CSP, the more reliant it becomes on the CSP for systems processing and data storage needs (which inevitably will grow over time). The cost of switching CSPs or returning to an internally managed solution increases as each year passes. In some cases, a CSP might recognize that the organization has become a captive renter once the internal technology staff has been disbanded and the CSP is solely supporting the important business processes. Annual price increases then become more likely.

- **Involvement of representatives across the organization** – Due to cloud computing's potential impact on many areas (e.g., technology, regulatory compliance, IT employees, and business operations), personnel from legal, internal audit, IT, and business processes should be involved in making cloud computing adoption decisions.

- **Clear definitions of responsibilities and required interactions between the organization and the CSP** – As part of its ERM program, management needs to be aware of potential control issues, legal issues, business operations issues, and IT issues that could arise with the engagement of a CSP. Roles and responsibilities of the organization and the CSP need to be clearly defined with respect to the following questions (refer to related information in "Appendix: Cloud Computing Governance – Roles and Responsibilities"):

  > Who in the organization or the CSP will be responsible for the cloud solution's compliance with laws and regulations?

  > Who in the organization will be responsible for managing the CSP relationship and monitoring the compliance of the CSP's service-level agreements?

  > Who in the organization is considered the owner of the contract with the CSP?

  > Who in the organization or the CSP will be responsible for designing, managing, and giving final approval for controls related to security, change management, and access rights within the cloud solution?

  > Since the organization is the ultimate owner of the data, who will be responsible for administering users and managing the data that is under the CSP's control?

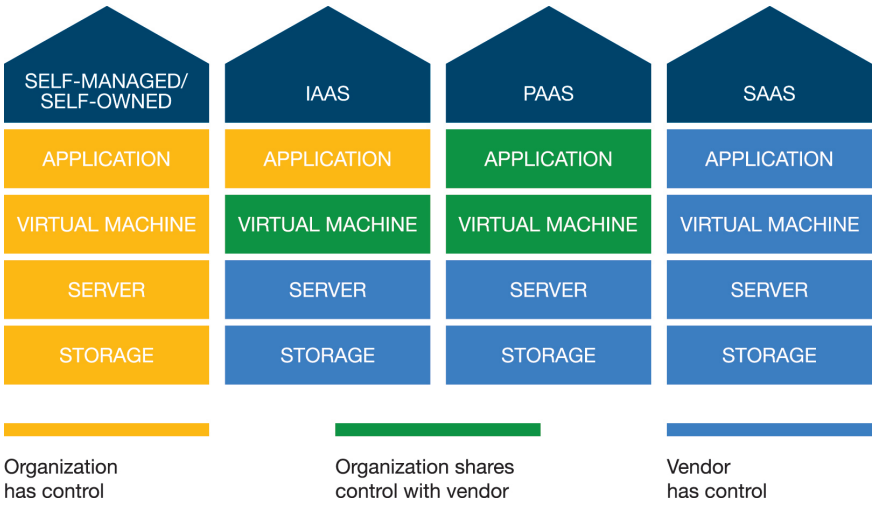
  > How will users be supported in the cloud solution?

  > Should users route issues and requests through the internal IT organization or directly to the CSP?

- **Evaluation of business continuity requirements** – The ability for the CSP to restore operations in the event of a disaster should be assessed and the contractual terms should clearly specify the CSP's obligations and financial liability if such an event should occur.

- **Relinquishment of direct control of specific technology areas** – The amount of control retained over the technology architecture is dependent on the selected cloud service delivery model. **Exhibit 7.1** illustrates the degree of control the organization retains over specific technology components (such as the application systems, virtual machine environments, servers, and storage) when comparing self-managed and self-owned facilities with the various cloud service delivery models.

Exhibit 7.1 Levels of Control by Cloud Service Delivery Model



- **Ultimate legal responsibility and liability** – By using public or hybrid cloud solutions, management has in effect assigned the performance of tasks to a third party but has not transferred its responsibility and liability for the risks and controls that affect the data and transaction processing. Specifically, with a public or hybrid cloud deployment model, the organization is outsourcing components of its infrastructure, software solutions, and related operations support. In most cases, the amount of liability and accountability a contract can transfer to a third party is limited.

Legal Ambiguity about Data Jurisdiction

An organization may be subject to multiple legal jurisdictions, depending on where the organization resides, the location of the cloud infrastructure, and where data is stored. At the time of this publication, significant ambiguity exists with respect to how the cloud computing paradigm fits in the international legal and regulatory environment. In addition, regulations such as HIPAA, national and regional data privacy laws, and the jurisdiction of law enforcement and other authorities further complicates the use of commercial public and hybrid cloud solutions.

As part of cloud computing governance and the organization's ERM program, management should consult with legal counsel to determine the related risks and challenges of complying with applicable laws if cloud computing solutions were to support some or all of the organization's processes. Some of the legal aspects of cloud computing that should be considered include:

> In what country is the data stored when the CSP's solution is in use?

> To what legal jurisdiction are the data and systems subject? Are there multiple jurisdictions?

> If the CSP stores data in a country different from the country of the organization and the organization's customers, what are the legal implications, and what are the organization's legal rights if a foreign court subpoenas the organization's or its customers' data?

> If a legal authority subpoenas the data of the organization's CSP or the data of a fellow cloud tenant can the organization's data be separated or isolated from the data that's being confiscated?

> What tax jurisdictions govern any transaction processing that is taking place?

> If a law enforcement agency seizes the CSP's server in its legal jurisdiction and it contains data about the organization's customers in a different legal jurisdiction, would the organization be violating the legal rights of its customers (and related data protection laws) for storing customer records in a public or hybrid cloud solution in the first place?

8. Conclusion

It has been proclaimed in some circles that cloud computing has as much potential to bring about change to organizations as the Internet did during the last decade of the 20th century. In time, cloud computing will establish its mark in the historical timeline of the evolution of technology.

The adoption and acceptance of cloud computing is congruent with the popularity and acceptance of other trends of the past decade (e.g., social networking sites and virtual retailing), for which the people and facilities cannot be seen but are greatly trusted to facilitate communications, store information, and transact business. A few decades ago, mainframe computers were locked up in a showcase center, and senior management took great pride during office tours to show off the elaborate physical security measures, the sheer size of the data centers, and the amount of equipment being used. The executives from that era felt confident that all of their organizations' information assets were stored in well-guarded facilities that could be easily verified. Today, with most of the available cloud solutions, the successors of this past generation of executives have a much cheaper technology option available in which they can neither tour the facilities (in many cases) nor have knowledge of the exact location of their organization's information assets.

Some of the unique aspects of cloud computing can pose new challenges to ERM programs. The apparent simplicity of adopting cloud computing belies how complex its management can become when risks materialize. It would be naïve to think that cloud computing will allow an organization to avoid adverse events – criminal activity, human error, and unforeseen accidents and disruptions – that can befall any type of organization. An effective cloud governance program is highly dependent on an accurate understanding of the risks combined with well-contemplated risk mitigation or acceptance strategies. By leveraging the COSO ERM framework, management will have an effective and consistent approach in identifying the universe of specific risks and risk responses that each cloud computing opportunity and decision entails.

Applying cloud computing solutions without the proper care, due diligence, and controls is bound to cause unforeseen problems. Used appropriately – with the necessary precautions and controls in place, as vetted by applying the COSO ERM framework – cloud computing could yield a multitude of benefits, some unheard of until now and some yet to be discovered. By being aware of the risks and other issues related to cloud computing, executives are more likely to achieve their organization's objectives as they manage the risks in this dynamic and evolving environment that likely will become the most popular computing model of the future.

Appendix: Cloud Computing Governance – Roles and Responsibilities

A strong ERM program to govern cloud activities requires senior management to take on additional responsibilities. The following describes the assignment of key cloud responsibilities:

Position	Responsibilities
Board of Directors	• Be aware of cloud computing trends and understand management's perspective on the impact of cloud to the industry and its business model • Be aware and have oversight of transformative IT projects such as cloud services • Understand how management is balancing risks with the benefits of cloud as part of its business and technology strategy • Leverage internal audit resources for assurance that cloud initiatives are in alignment with the organization's risk appetite and controls philosophy
Chief Executive Officer	• Define the organization's point of view and policies regarding outsourcing • Understand the impact cloud computing is having on the organization's industry • Be aware of where and how the organization is using cloud computing
Chief Financial Officer	• Provide new disclosures regarding cloud usage in financial reporting • Evaluate and monitor the total cost of ownership and return on investment with cloud computing • Evaluate tax and accounting benefits of cloud computing versus alternatives • Implement policies and controls over procurement of cloud services • Monitor the financial health of each third-party CSP
Chief Legal Officer	• Ensure that the organization's cloud activities comply with laws and regulations • Monitor for new laws and regulations that would impact the organization's cloud solution or its CSP and establish a plan for compliance • Review and approve cloud services procurement policies • Provide input on data classification policies and processes • Review CSP contracts and ensure protection of the organization's interests and rights • Understand the legal jurisdiction aspects of the organization's operations as they relate to using cloud services hosted in different countries

Position	Responsibilities
Chief Information Officer	• Understand and monitor cloud computing's potential to support current business strategies and new business opportunities • Establish overall strategy for leveraging and aligning cloud solutions • Facilitate the integration of cloud solutions into the organization and with the current IT infrastructure • Assist with incorporating cloud governance into the organization's ERM program • Implement a data classification scheme in conjunction with data owners • Establish cloud processes for resource provisioning, user access management, and change management • Establish the organization's cloud incident management program • Monitor and enforce CSP service-level agreements • Monitor activities of the CSP and fellow cloud tenant customers
Chief Audit Executive or Internal Auditor	• Perform periodic audits to evaluate the design and effectiveness of the blended control environment in which controls and processes are shared with the CSP • Audit the CSP or review SOC reports to verify the effectiveness of CSP controls relied upon by the organization • Perform periodic compliance audits of data residing on external clouds to verify compliance with data classification polices • Audit CSP spend and contractual compliance • Evaluate cloud governance

About COSO

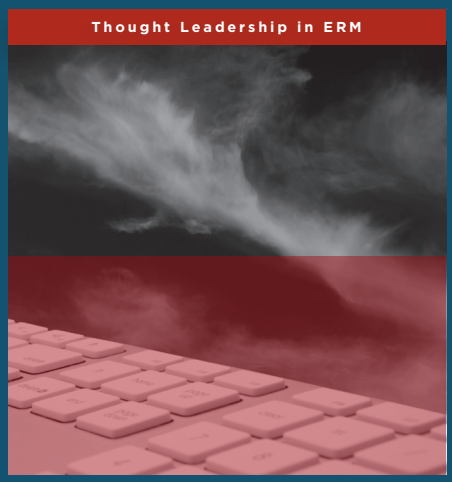
Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

About the Authors

Crowe Horwath LLP – Crowe Horwath LLP (www.crowehorwath.com) is one of the largest public accounting and consulting firms in the United States. Under its core purpose of "Building Value with Values®," Crowe assists public and private company clients in reaching their goals through audit, tax, advisory, risk, and performance services. With offices coast to coast and 2,500 personnel, Crowe is recognized by many organizations as one of the country's best places to work. Crowe serves clients worldwide as an independent member of Crowe Horwath International, one of the largest networks in the world. The network consists of 150 independent accounting and management consulting firms with offices in more than 580 cities around the world.

The contributing authors from Crowe Horwath LLP are Warren Chan, principal; Eugene Leung (formerly of Crowe); and Heidi Pili (formerly of Crowe).

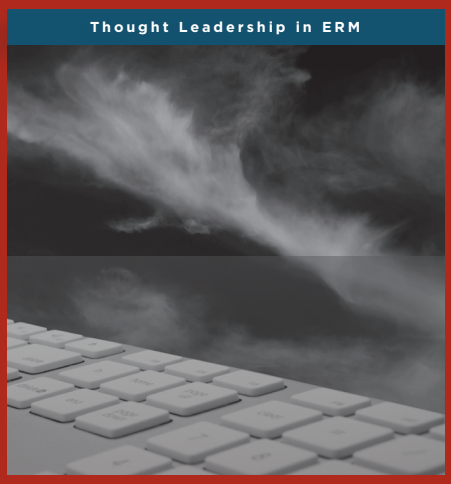
Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction.



COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org



ENTERPRISE RISK MANAGEMENT FOR CLOUD COMPUTING

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org