COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

ENTERPRISE RISK MANAGEMENT FOR CLOUD COMPUTING

By

Crowe

Mike Grob | Victoria Cheng

July 2021

Authors

Mike Grob
Principal, Consulting
Crowe LLP – Chicago

Victoria Cheng
Managing Director, Consulting
Crowe LLP – Chicago

COSO Board Members

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence.
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)

COSO
Committee of Sponsoring Organizations of the Treadway Commission

coso.org

Enterprise Risk Management

ENTERPRISE RISK MANAGEMENT FOR CLOUD COMPUTING

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

July 2021

1234567890 PIP 198765432

Design and production: Sergio Analco.

Contents

INTRODUCTION

Since the first introduction of cloud computing, the cloud has grown and expanded. Prior to the 2020 COVID-19 pandemic, in April 2019 Gartner valued it as a $214 billion market in 2019 with anticipated growth of 16.5% to $250 billion in 2020 and 15.7% to $289 billion in 2021[4]. Based on the pandemic and the need for remote work, the expansion of cloud computing was faster and accelerated the implementation timeline for many organizations. A year and a half later, in November 2020, Gartner reported worldwide public cloud service revenue was $243 billion in 2019, estimated a 6% increase to $258 billion in 2020, and projected an18% increase to $305 billion in 2021[5]. These represent a 3% increase in 2020 estimates and 5.5% increase in 2021 estimates a year and a half later.

Leveraging cloud computing in some industries may have been a strategic advantage at one point. What the pandemic brought to light was the need for more remote and flexible work environments and the IT infrastructure to support the organization in that effort. Utilizing cloud computing has become an essential element to compete in the marketplace.

The speed at which cloud computing can be procured and implemented is one of its many valuable traits. However, facing the inertia of accelerated access to cloud based capabilities, some organizations may not have had the capacity to implement appropriate controls designed to mitigate the risks in their cloud environments.

There are several definitions of cloud computing

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]"

- ***National Institute of Standards and Technology (NIST)***

. . .

"Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.[2]"

- ***International Organization for Standardization (ISO)***

. . .

"The practice of storing regularly used computer data on multiple servers that can be accessed through the Internet.[3]"

- ***Merriam-Webster***

. . .

In the simplest terms, **cloud computing is a computing model that utilizes pooled resources over the internet**. The management of the underlying servers and processes may be outsourced to another organization.

1 The NIST Definition of Cloud Computing Special Publication 800-145 – September 2011 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

2 ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary – October 2014 https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en

3 Merriam-Webster

4 https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

5 https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Internal Control – Integrated Framework* (2013) and *Enterprise Risk Management – Integrating with Strategy and Performance framework* (2017) provide a comprehensive foundation for governance and control of cloud computing and cloud security. The COSO Enterprise Risk Management (ERM) framework provides a construct for organizations to establish governance, identify and respond to risks, monitor performance, maintain communications, and adjust as there are changes to the organization or its business objectives, or to the industry or its environment. The COSO Internal Control framework also provides a tool to use, typically in the performance component of the COSO ERM framework, to assess risks and risk responses.

The purpose of this publication is to provide a guide to establishing cloud computing governance leveraging COSO's frameworks. We also provide a roadmap to implement cloud computing (Appendix A. Roadmap to Cloud Computing) and describe appropriate roles and responsibilities (Appendix B. Roles and Responsibilities). This publication acknowledges that many organizations will have a hybrid IT environment (using both in house/on-premise IT resources as well as cloud computing resources). This publication will focus solely on cloud computing considerations.

Organizations are at various points of maturity in adopting and implementing cloud computing. Those at initial stages will benefit from this guidance. Those who have completed an implementation can still use this guide to evaluate and, when needed, retroactively implement enhanced governance and controls. Bolstering cloud governance will reduce the organization's risk and allow for more efficient and effective use of cloud computing and monitoring in a multi-cloud environment.

ENTERPRISE RISK MANAGEMENT WITH A CLOUD COMPUTING ENVIRONMENT

A cloud computing environment is complex, whether deployed in a public, private or hybrid cloud environment. Its management is equally complex as it requires integration of numerous operating functions with a web of third party service providers. Similarly complex is the integration of cloud governance within the holistic ERM process and framework an organization uses.

The 2004 COSO Enterprise Risk Management Framework was updated to the 2017 COSO Enterprise Risk Management – Integrating with Strategy and Performance to focus on the importance of identifying and addressing risk in strategic settings and in driving an organization's performance. With this update, organizations are provided a robust framework that applies to the governance and management of their cloud computing environment.

Diagram 1. **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework***

2017 COSO Enterprise Risk Management – Integrating with Strategy and Performance

An organization's management is responsible for managing the risk to the organization. Management must incorporate the board and key stakeholders into the ERM program so that risk management is integrated with the organization's strategy and business objectives. Effective ERM involves multiple departments and functions; it should be integrated into the strategy of the organization and embedded into its culture. Successful ERM goes beyond internal controls to address governance, culture, strategy, and performance. Effective cloud computing and cloud enterprise risk management is integrated within the organization to support the organization's strategy and objectives, align with the culture, and enhance value.

The COSO Enterprise Risk Management framework itself is a set of principles organized into five interrelated components:

1. Governance and Culture: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

2. Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

3. Performance: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

4. Review and Revision: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

5. Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.[6]

Diagram 2. **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework* – 20 Principles tied to the 5 Components**

2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*

The following chapters explain how to apply the COSO *Enterprise Risk Management – Integrating with Strategy and Performance framework* by evaluating each component as well as the 20 principles to cloud computing governance followed by guidance on how to apply the principles to cloud computing. This guide provides a structure to utilize the COSO ERM framework in thinking through cloud computing risks. Cloud computing strategy, risks, and ERM should be embedded in the overall ERM program within an organization, as cloud computing is another tool to help an organization achieve its business strategy and create value.

6 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*

GOVERNANCE AND CULTURE

Table 1.1 **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework* – Governance and Culture Principles**[7]

Principle	Description
1. Exercises Board Risk Oversight	The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. Establishes Operating Structures	The organization establishes operating structures in the pursuit of strategy and business objectives.
3. Defines Desired Culture	The organization defines the desired behaviors that characterize the entity's desired culture.
4. Demonstrates Commitment to Core Values	The organization demonstrates a commitment to the entity's core values.
5. Attracts, Develops and Retains Capable Individuals	The organization is committed to building human capital in alignment with the strategy and business objectives.

1 Exercises Board Risk Oversight

An organization's governance and culture begin with its board of directors and management. While management defines its business objectives and culture, the board of directors should provide oversight to the strategy and objectives. A diverse board with members who collectively have a broad spectrum of knowledge within the industry, the organization, technology, governance and compliance, and finance, is needed to provide the necessary expertise to monitor management's activities to realize the organization's business objectives.

The board of directors should use their oversight role to ask questions of the organization related to:

- how technology can help the organization achieve its objectives,
- how technology may increase or decrease an organization's risk (including third party risk),
- what are the current and future cloud trends and industry technology shifts,
- what is the impact of cloud computing to the organization (including retirement of on-premise infrastructure),
- how does the organization's strategy align with its cloud service provider's strategy, and
- how does the organization compare to its peers and benchmarks.

7 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*

2 Establishes Operating Structures

Before an organization migrates to cloud computing, the organization needs to define the framework and governance. The organization should have organizational structures in place to support its business objectives. These organizational structures should be looked at for how they could support cloud computing (i.e., will there be additional roles defined, will there be dotted line reporting, where is the responsibility?).

To create the necessary governance structures, the organization may decide to put together a Cloud Computing Steering Committee to ensure proper oversight is given over what processes, applications and data migrate to cloud computing. This Cloud Computing Steering Committee should ensure appropriate cloud governance structures are in place, such as policies, procedures, oversight to avoid shadow IT (IT resources that are not approved by the IT department), and an organizational structure to monitor cloud computing performance. Ongoing, the Cloud Computing Steering Committee can reinforce lessons learned and reinforce the risk culture.

Cloud computing activities will affect multiple areas within the organization. For example, Legal, Finance, Information Technology, Risk, Vendor Management, Compliance, Internal Audit, and all impacted operational departments, should work collaboratively with transparency over the cloud computing adoption and monitoring processes.

Additionally, the organization needs to work with its cloud service providers (CSPs) to define the operating structure and responsibilities for the organization, its CSP, and its CSP's CSP, if applicable. For example, if a software as a service (SaaS) cloud service provider uses operating system and database services from an infrastructure as a service (IaaS) provider, the organization's CSP, the SaaS company, also has a CSP, the IaaS company. Clear roles and performance measures between vendors is essential to good governance.

A defined responsibility assignment matrix, such as a RACI (responsible – accountable – consulted – informed) matrix, applied to the assigned personnel, creates accountability and communication as well as the open, forward thinking, collaborative culture the organization seeks to achieve with cloud computing. Open communication channels and proper involvement of individuals at each RACI level enhances the understanding and entrenching of a risk mindset into the culture of the organization. See Appendix B – Roles and Responsibilities for major roles needed in cloud computing.

3 Defines Desired Culture and 4 Demonstrates Commitment to Core Values

Creating a cloud-aware culture throughout the organization is necessary to enforce governance consistently across the organization. Management sets the tone for cloud culture, usage, data privacy, data security, and cyber security. Cloud computing may be utilized in any department within an organization; therefore, it is necessary for all personnel to understand their role and the enterprise risks related to cloud computing. A cloud computing lens needs to be integrated into cross functional planning processes to ensure transparency. Viewing cloud computing as part of a holistic strategy, versus each department finding an independent solution to meet a business need, is essential to a good cloud governance model. Defining accountable individuals demonstrates the organization's commitment to core values.

Another factor is understanding the culture and value of the CSP partners. Utilizing a CSP makes them an extension of the organization. Understanding this relationship and selecting appropriate partners will reflect and enforce the organization's culture and core values.

5 Attracts, Develops and Retains Capable Individuals

As part of its human capital management, the organization should identify the internal resources needed to manage cloud governance. Appropriate training should be developed and provided so employees can properly operate in a cloud computing environment. Some cloud computing tasks can be incorporated into existing functions with some additional training and nuances for differences in cloud computing. End user roles will be different than those responsible for cloud vendor management, or user administration. Regardless of the role, the organization's culture and values should show through in establishing the framework for cloud computing governance.

The utilization of a CSP shifts certain responsibilities for technology to the CSP organization; likewise, it shifts the human capital management to the CSP. Understanding the CSP's approach to human capital management and how it complements the organization's capabilities is a way to look at cloud computing human capital management as part of the holistic ERM process.

Table 1.2 **Key Activities for Cloud Computing – Governance and Culture Principles**

Principle	Description	Cloud Computing ERM Key Activities
1. Exercises Board Risk Oversight	The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.	Board of directors understands cloud computing, trends, and potential impact on the organization and industry.
2. Establishes Operating Structures	The organization establishes operating structures in the pursuit of strategy and business objectives.	The organization establishes a Cloud Computing Steering Committee to oversee the migration and implementation of cloud computing.
3. Defines Desired Culture	The organization defines the desired behaviors that characterize the entity's desired culture.	Executive management defines the cloud usage culture and how cloud computing can be utilized to support the organization's mission, vision, core values, strategy, and business objectives.
4. Demonstrates Commitment to Core Values	The organization demonstrates a commitment to the entity's core values.	The Cloud Computing Steering Committee promotes cloud governance accountability through communication and follow-up.
5. Attracts, Develops and Retains Capable Individuals	The organization is committed to building human capital in alignment with the strategy and business objectives.	The organization defines the necessary talent and identifies, attracts, trains, develops, manages, rewards, and retains diverse individuals capable of building an inclusive environment who perform and manage cloud governance activities throughout the organization.

STRATEGY AND OBJECTIVE-SETTING

Table 2.1 **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework* – Strategy and Objective Setting Principles**[8]

Principle	Description
6. Analyzes Business Context	The organization considers potential effects of business context on risk profile.
7. Defines Risk Appetite	The organization defines risk appetite in the context of creating, preserving and realizing value.
8. Evaluates Alternative Strategies	The organization evaluates alternative strategies and potential impact on risk profile.
9. Formulates Business Objectives	The organization considers risk while establishing the business objectives at various levels that align and support strategy.

6 Analyzes Business Context

While cloud computing offers ease of entry and quick changes, prior to migrating to the cloud an organization should formally define its overall cloud computing strategy and objectives for moving to the cloud. There are many reasons to move some or all of the IT environment to the cloud, but to obtain benefit and value, an IT organization must work with the business functions to understand the goals and strategy and help create a cloud computing strategy that supports the business. This cloud strategy should be vetted with management as well as other stakeholders, such as board members, to assess other influences and direction.

Per the 2017 ERM framework, business context includes the "trends, events, relationships and other factors that influence, clarify or change the company."[9] The COVID-19 pandemic changed the business context for many organizations. As a result, many companies needed to quickly change their cloud computing strategy to enable employees to remotely access systems and data. Microsoft CEO Satya Nadella expressed in April 2020, "We've seen two years' worth of digital transformation in two months."[10]

The cloud strategy will also focus on the opportunities related to cloud computing, such as the ease of use with intuitive user interfaces, fewer customizations, faster speed of deployment, and easier scalability. These all enable innovation and digital transformation which allow the organization to quickly pivot and support new business objectives.

In a more established organization without major changes in business objectives, the cloud strategy may be focused on efficiency – with easier maintenance for the IT department, and cost savings due to only using storage and computing that is needed vs. maintaining for peak capacity.

The cloud strategy includes what is needed to support the organization, its objectives, and its growth. The underlying mission, vision and values for the organization, and its "why," is reflected in the cloud strategy. The cloud strategy provides guidance for infrastructure and application migrations and acquisitions.

8 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*
9 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*
10 https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

The cloud strategy may include a multi-cloud strategy, multiple cloud deployment models, and multiple cloud delivery models. (See Appendix C. Glossary and Definitions) Additionally, the cloud strategy may be a multi-year roadmap, so the immediate strategy and approach versus the end result will look different, with different risks and potentially different vendors used along the way.

The cloud strategy and the use of CSPs will affect the organization's risk profile which will need to be analyzed. Different CSPs, due to their ERM governance, their vendor's ERM governance, and their customers' ERM governance, may have different impacts to the organization's risk profile.

7 Defines Risk Appetite

Once the cloud strategy is determined, the organization must evaluate the risks to that strategy and assess whether its risk appetite is affected. This understanding will help the organization determine the appropriate outcome of detailed cloud computing scenario assessments to inherent and residual risk and likelihood and impact assessments based on different cloud deployment models, cloud delivery models, or specific CSPs during the ERM Performance component. For example, part of a hybrid IT environment may include the use of in-house managed application for data analytics over sensitive data, while an enterprise resource planning (ERP) application is on a cloud SaaS, and devops (a combination of development and IT operations) on a private PaaS (platform as a service). Management's analysis of inherent risk and residual risk would allow the organization to choose the appropriate IT environment for the organization.

As illustrated in the ring in Diagram 3 below, a cloud strategy can create risk to the organization. It is possible the cloud strategy does not align with the business strategy, or there could be new risks to the execution of the business strategy due to the use of cloud computing. For example, the cloud strategy and cloud applications may only support a subset of the organization's products or service lines. There could be other implications from the cloud strategy, such as, concentration at one CSP, resulting in potential vulnerabilities or a higher risk profile. When these are properly managed and addressed, the organization will enhance performance.

The organization needs to define its risk appetite as it regards the cloud strategy. The organization may determine that its risk appetite for different types of data is different, e.g., employee personally identifiable information (PII) is different from customer data where the customer is another business organization. Similarly, the organization may have different availability requirements and recovery time objectives for different applications, e.g., an ordering system may have a higher requirement than a training system. With this knowledge and understanding, the organization can assess what is suitable for a cloud computing strategy and its cloud strategy may differ for different parts (e.g., business units, departments) of the organization depending on the risk appetite related to those processes.

Diagram 3. **COSO Enterprise Risk Management in the Context of Mission, Vision, Core Values, and as a Driver of an Entity's Overall Direction and Performance**

2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*

8 Evaluates Alternative Strategies

Defining the initial cloud strategy allows the organization to objectively review alternatives and assess them under the lens of "creating, preserving, and realizing value."[11] As various cloud strategy, and cloud delivery and cloud deployment models are reviewed, the organization should look at its risk profile, its ability to achieve business objectives, and how those objectives eventually drive growth, productivity, efficiency, and value.

Something to consider as the organization thinks through and evaluates alternative strategies, is how that strategy will impact its innovation opportunity. Traditional on-premise systems have been known to accumulate what is referred to as technology debt. Technology debt can be summarized as the cost to maintain existing systems plus opportunity cost of not prioritizing modern systems.

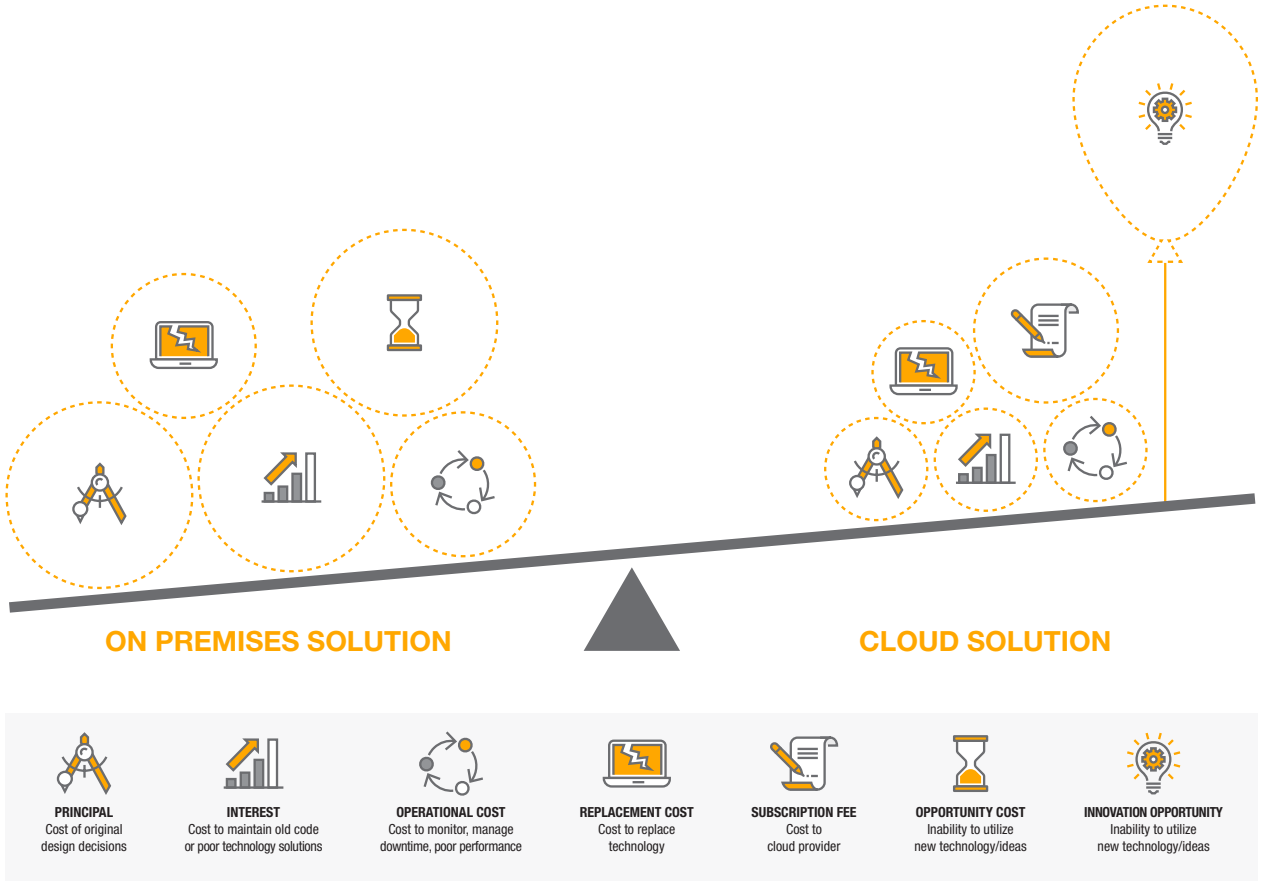
Common sources of technology debt include:

- **Overly customized packaged software** – implementing an ERP system that is heavily customized can inhibit an organization's ability to take updates from the software vendor.
- **Poor technical solutioning** – selecting the shorter or more familiar approaches to addressing a business requirement when there is a more strategic long-term option.
- **Obsolete technology** – outdated operating systems, software packages and infrastructure.

Organizations with a high amount of technology debt typically have increased risks and higher costs (both to maintain and retire debt. To determine the appropriate course of action, organizations must weigh the costs that contribute to higher technology debt (as illustrated in Diagram 4), against the alternatives that would retire the debt. Similarly, organizations who have not invested effectively in technology may have increased risks and higher costs due to lost efficiency and effectiveness related to technology deployment and related matters.

As organizations evaluate cloud alternatives and review their technology debt, they should balance the costs against changing processes to fit a specific application's functionality, time to implement an alternative solution, additional cyber security risks due to multi-tenancy.

Diagram 4. **Elements Contributing to Technology Debt vs Alternative Costs**



11 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*

9 Formulates Business Objectives

Once the cloud strategy is defined, cloud objectives should be defined to support the business objectives. The cloud objectives should include a cloud security model as part of cloud governance.

Business strategies and objectives are updated as the organization grows or in reaction to external events. These updates drive continued evaluation of the cloud strategy within the context of the ERM framework. Additionally, risk appetite can change over time and should be regularly updated as well.

Table 2.2 **Key Activities for Cloud Computing – Strategy and Objective Setting Principles**

Principle	Description	Cloud Computing ERM Key Activities
6. Analyzes Business Context	The organization considers potential effects of business context on risk profile.	The organization assesses the impact of different cloud strategies (cloud deployment models, cloud delivery models, etc.) on the achievement of the strategy and business objectives.
7. Defines Risk Appetite	The organization defines risk appetite in the context of creating, preserving and realizing value.	The organization defines its risk appetite for cloud governance addressing cloud risks such as data privacy, access, reliability, compliance, and cyber security.
8. Evaluates Alternative Strategies	The organization evaluates alternative strategies and potential impact on risk profile.	The organization considers alternative cloud strategies and impact on business objectives.
9. Formulates Business Objectives	The organization considers risk while establishing the business objectives at various levels that align and support strategy.	The organization defines cloud objectives to support business objectives .

PERFORMANCE

Table 3.1 **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework* – Performance Principles**[12]

Principle	Description
10. Identifies Risk	The organization identifies risk that impacts the performance of strategy and business objectives.
11. Assesses Severity of Risk	The organization assesses the severity of risk.
12. Prioritizes Risks	The organization prioritizes risks as a basis for selecting responses to risks.
13. Implements Risk Responses	The organization identifies and selects risk responses.
14. Develops Portfolio View	The organization develops and evaluates a portfolio view of risk.

10 Identifies Risk

Cloud computing risk can come from the internal or external environment and can impact strategic, financial, operational, compliance, and/or reporting objectives. It is critical to identify risks that will affect the performance and achievement of the cloud computing strategy and thereby, the achievement of business objectives and the creation of value.

When an organization adopts cloud computing, it is shifting one or more IT responsibilities to an outside party. There is great upside to this approach, given that most organizations can find a strategic partner who performs these responsibilities as their core competency. However, although delegating these responsibilities moves where they are performed, it does not remove the risk. Risk (and responsibilities for mitigating such risk) will vary depending on the deployment model. One could argue that the most common risk an organization can make is misconceiving what party owns the controls for a given risk. The organization responsible for a control affects the risk impact for the organization.

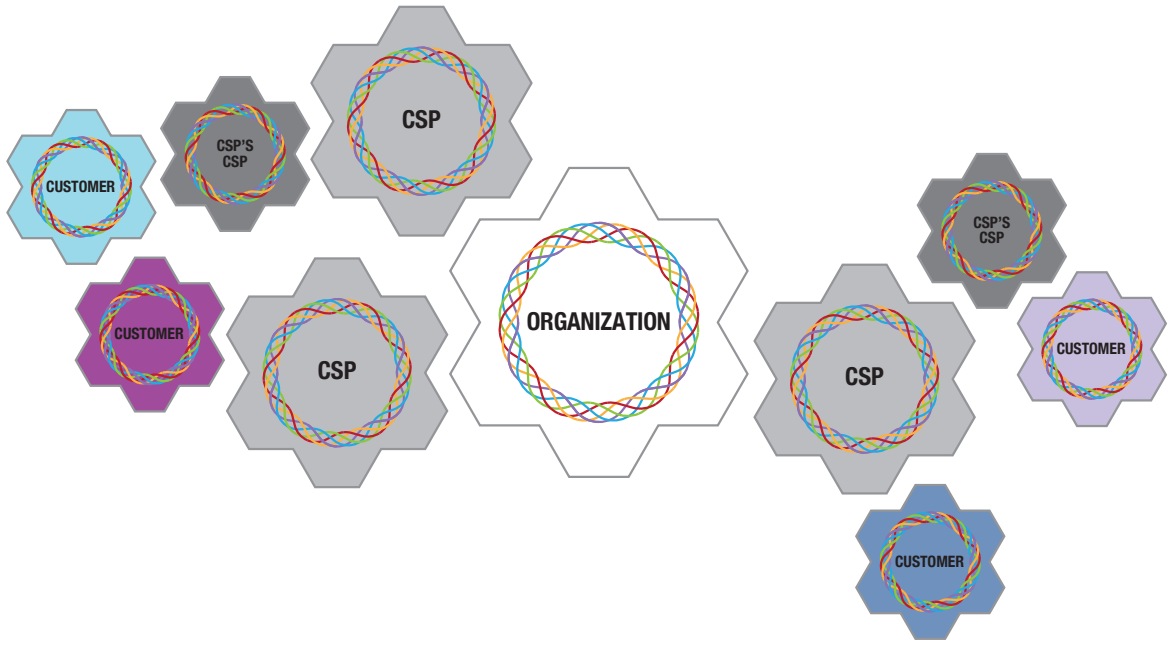
Gartner estimates that by 2025, 99% of cloud security failures will be the fault of the customer.[13] Organizations should no longer be questioning if the cloud is secure enough for them. The more appropriate question to ask is: "Is the organization using the cloud securely?"

Organizations can transfer some activities to their cloud service providers, but they cannot transfer all their risk. For example, if their cloud service provider does not perform an agreed upon activity, such as patching, and that vulnerability was utilized to breach the organization's data, the organization will still need to handle the fall out and breach of trust of its customers and the lost data, even if the organization wasn't directly at fault.

When using a CSP, the organization's risk profile becomes intertwined with that of the organization's cloud vendor. In a multi-cloud environment, the use of multiple cloud vendors complicates and entangles the ERM framework with that of many other vendors as illustrated in Diagram 5. Additionally, some CSPs will use another CSP for support, thus enmeshing even more vendors. Many organizations have a multi-cloud environment and use multiple CSPs. What happens at one organization may have an impact on another organization. For example, a cloud outage at a PaaS will affect a SaaS CSP that utilizes the PaaS for its underlying infrastructure.

12 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*
13 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

Diagram 5. **COSO Enterprise Risk Management Integrating with Strategy and Performance Framework – With Organization and CSP Represented**

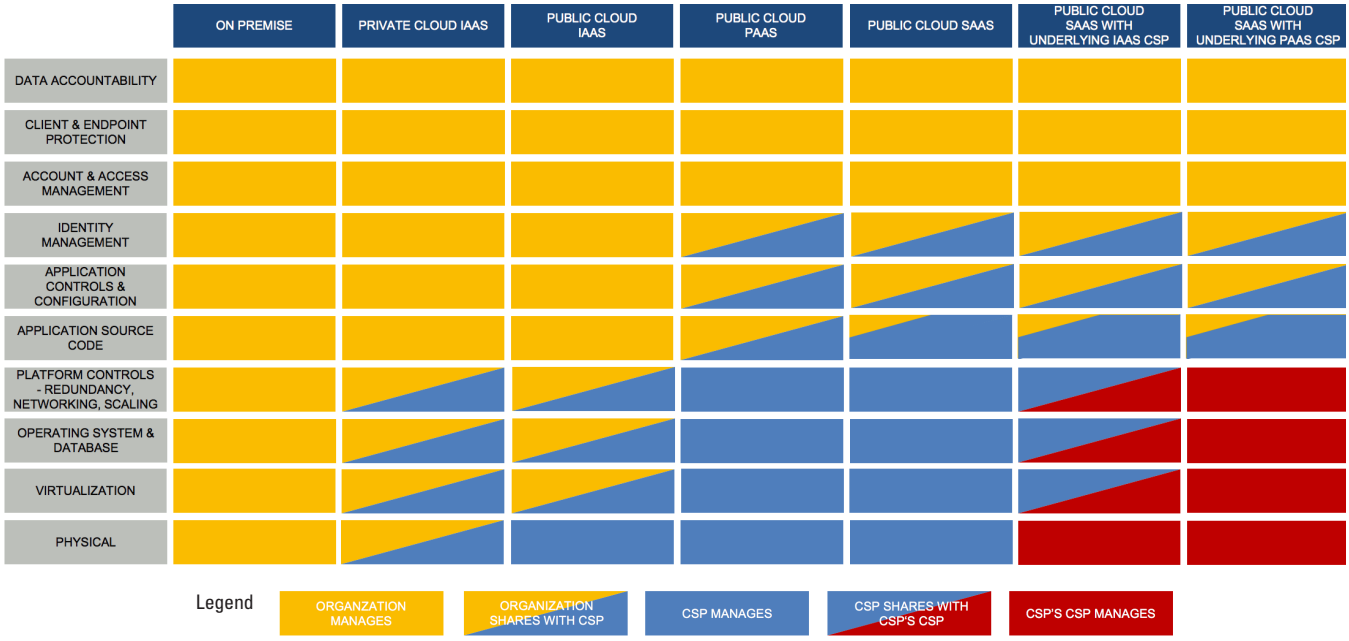


Misunderstanding Responsibility

Some form of delegation is expected in all cloud environments. As illustrated in Diagram 6, there is shared responsibility in many cloud delivery and cloud deployment models. However, many organizations underestimate the responsibilities that they still own or share with the CSP. This is particularly important when dealing with IaaS and PaaS models but is also prevalent with SaaS. It is important to remember that while organizations can shift responsibility, they cannot outsource their risks. Here are some questions to highlight common areas of misconception.

- What portion of the environment is **multi-tenant**?
  To a certain extent, sharing exists in all cloud environments. The important thing is to understand what is shared and who controls the boundaries. Multitenancy can mean a lot of different things.
- What **access controls** is the organization responsible for managing?
  All cloud deployment models require that some level of access controls is managed by the subscribing organization. There is often shared responsibility (between the organization and the CSP) for areas such as firewalls, VPNs (virtual private networks) and multifactor authentication. CSPs who provide these capabilities often leave configuration and enforcement up to the subscribing organization.
- To what extent is infrastructure **redundancy** managed by the cloud provider?
  Organizations should not make the broad assumption that all aspects of the cloud are redundant by default. The cloud service provider indeed owns a significant portion of the responsibility, but depending on the deployment model, ownership may lie with another party.

Diagram 6. **Responsibility by Cloud Deployment Model and Cloud Service Delivery Model**



11 Assesses Severity of Risk and 12 Prioritizes Risks

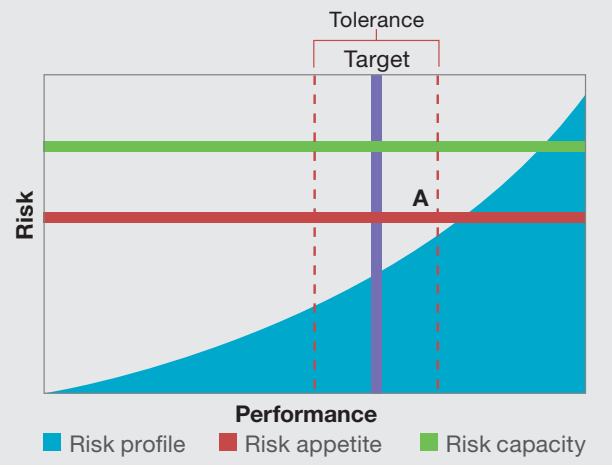
Once identified, cloud computing risks should be prioritized and assessed for severity. Assessment can be qualitative and quantitative and should account for risk impact and risk likelihood. Additionally, it should be assessed at multiple points in time and throughout the organization for different types of data. For example, the same risk, user access, may have different severity depending on what the cloud application is and what the cloud deployment and delivery model is such as the difference between a custom application managed on a private IaaS cloud versus a public SaaS application managed by a CSP with an underlying PaaS CSP supporting it.

When evaluating specific CSPs, cloud deployment models, and cloud delivery models, the organization defines the risks, assesses the risks, and prioritizes the risks prior to selecting an approach and vendor. Once the CSP is determined, appropriate risk responses are created to address the specific risks and scenarios presented by the CSP. Risk responses include acceptance, avoidance, pursuit, reduction, and sharing.

13 Implements Risk Responses

Risk responses are implemented and evaluated to assess the residual risk and to determine where the organization falls within its risk appetite and risk capacity. As illustrated in Diagram 7, the goal is to fall within the risk tolerance.

Diagram 7. **COSO ERM – Risk Profile**



2017 COSO Enterprise Risk Management – Integrating with Strategy and Performance

While there are five primary risk responses, the main one for cloud computing will be reduction.

- **Accept** – Accepting cloud computing risks is possible in certain scenarios where the organization may feel constrained, such as accepting the risk profile of other fellow cloud tenants. The organization must evaluate this against their risk tolerance thresholds.
- **Avoid** – Generally, avoidance may only work in certain situations, such as, the organization selects a nation based PaaS versus an international PaaS to address specific data privacy requirements, the organization decides certain data types, such as intellectual property, cannot be posted to a public cloud, or the organization implements a full private cloud solution. Even with these scenarios, there will still be some additional risks that will arise and need to be addressed through reduction and mitigation.
- **Pursue** – When migrating to the cloud, additional opportunities are generated to create, preserve and realize value for the organization frequently by allowing the organization to further innovation and digital transformation and increase efficiencies.
- **Reduce** – Incorporating additional cloud governance and monitoring controls can reduce risk. This is the most common risk response for cloud computing to mitigate the inherent risks within technology along with the additional risks brought onto the organization using cloud computing and outsourcing to CSPs.
- **Share** – There is a limit to which sharing is an appropriate response for cloud computing. There are few risks, such as cyber breaches, that can be addressed to some extent through buying cyber insurance and thus sharing the risk. However, the primary risks of cloud computing cannot be shared.

Use of the 2013 COSO *Internal Control – Integrated Framework* is one approach to structure and develop the risk reduction responses for cloud computing risks. It is also critical to recognize the integration of the organization's internal control framework and that of the CSPs as illustrated in Diagram 8. The CSP's internal controls (as represented by the cubes within the larger cube) become a part of the organization's internal controls (as represented by the larger cube). In all cloud delivery models, a portion of processes and controls will be outsourced to the CSP. The organization relies on the CSP to perform those internal controls. The organization needs to understand and review the CSP's control design to ensure it adequately addresses the risk, and also monitor the effective execution of the controls.

Diagram 8. **2013 COSO *Internal Control – Integrated Framework*[18]– With Organization and CSP Combined View**

The Performance component of the COSO Enterprise Risk Management – Integrating with Strategy and Performance focuses on risk responses. The following expands on a few recommended responses for typical cloud computing risks.

18 2013 *COSO Internal Control – Integrated Framework*

RISKS – Reliability and vulnerability

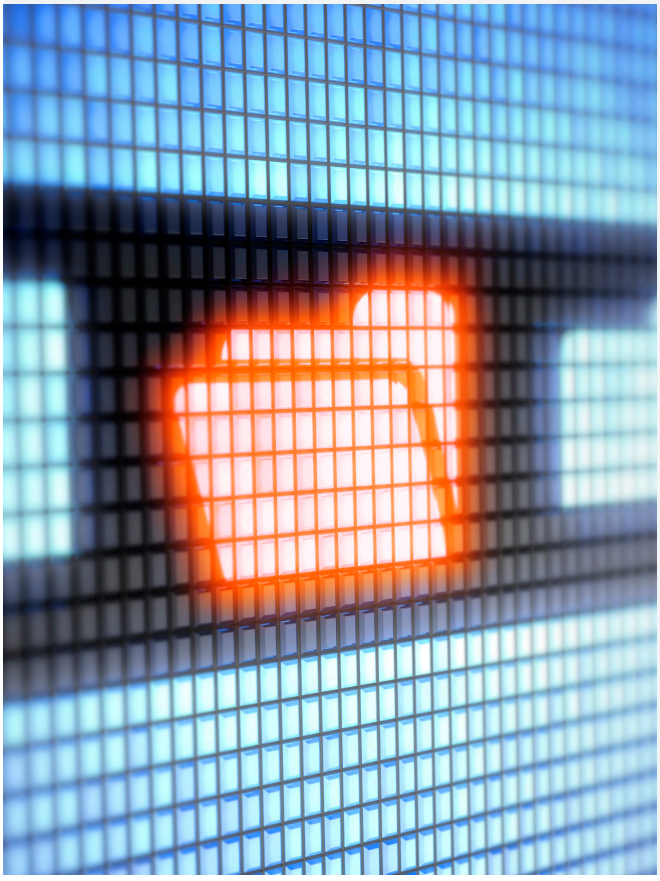
RESPONSE
Performance monitoring, security monitoring, and incident response

An organization should first seek to partner with a CSP with high reliability. Then the organization needs to monitor its CSP for performance and up time.

In most cloud delivery models, the CSP will manage the infrastructure and should be performing security and vulnerability assessments. The output of these assessments and how the CSP responds and remediates any issues should be shared with and monitored by the organization.

The CSP should have appropriate incident response measures in place to identify their own incidents. Additionally, the CSP should have processes in place for the organization to report incidents to them and for the organization to track progress on their incidents. Since the management of the application and service is coupled, the incident response should be coupled as well.

RISKS – Multi-tenancy, data leakage, and data theft



RESPONSE
Data classification, data destruction, security

In the case of public cloud and multi-tenancy, there is a higher risk of data theft or leakage. The organization should thoroughly assess what data can be adequately secured if put on the cloud. Performing a data classification exercise to categorize and assess data risks can help to define parameters and what data (along with what applications) should be put on what type of cloud deployment model and cloud delivery model. The organization should assess how much control they want to have over the data.

Beyond a data classification policy, the organization should also enforce a data destruction policy. This way the organization does not keep excessive, or potentially outdated data in the cloud. Maintaining personal data in the cloud for analytics may decouple the data from notice requirements and enable the organization to use personal data outside of expressed permissions which may violate privacy regulations.

Security around the data can be gained through the implementation of secure access service edge (SASE) solutions. SASE includes networking and security components such as secure web gateways, CASB (cloud access security broker), advanced threat protection, and zero trust network access. SASE includes network security mechanisms that provide a layer of connectivity and security to apply the organization's security policies between the on-premise or remote users and devices to connect to the cloud.

RISKS – Single points of failure

RESPONSE
Redundancy, business continuity plans, and incident response

As all data and transactions will need to pass through the internet in a cloud computing environment, there is the single point of failure in the connection. An organization should look at what redundancy options are available in a cloud computing environment so traffic can be rerouted, if needed. When implementing a cloud tool, an organization should design for failure. Additionally, an organization should have business continuity plans in place including short term and medium-term work arounds.

Consistent with the risk of general system reliability, the incident response process is critical to getting back online.

RISKS – Compliance

RESPONSE
Monitor internal and external environment, vendor monitoring

Regulations evolve and organizations change over time. Therefore, an organization's regulatory compliance needs also change. An organization needs to monitor its internal environment to understand the changes the organization has undertaken and the impact on its compliance requirements. Likewise, the organization needs to monitor its external environment to assess additional or changing compliance requirements. Additionally, the organization needs to monitor its CSP vendors to assess the compliance capabilities of the CSP and what, if any, additional steps the organization must perform in order to become compliant.

RISKS – Cyber attacks

RESPONSE
Incident management

There are many types of cyber security threats to cloud computing. The most common include malware injections, denial of service (DoS), API attacks, and access hijacking. The use of open source technology may increase the risk to cyber-attacks as vulnerabilities are common knowledge. While cyber security is a risk to both on-premise and cloud computing, there is an additional risk due to multitenancy. The multi-tenant model could make an organization a higher value target.

The organization needs to understand the processes the CSP has to monitor and detect potential threats and how they take action. Additionally, the organization needs a mechanism to notify the CSP of incidents and manage incidents with the CSP.

RISKS – Shadow IT

RESPONSE
Policies and procedures and security prevention tools

Policies and procedures to establish expectations with employees on what are allowable cloud computing services and vendors, who can procure services, and what data can be moved to the cloud can provide a framework to reduce unauthorized cloud activity.

Additionally, firewalls, proxy servers, and web filters, can further reduce the amount of shadow IT being used in an organization. These configurations need to be consistently maintained and applied in order to be effective as new software and websites are released. Organizations can also configure data loss prevention tools to monitor and restrict data from exiting the organization.

Table 3.2 summarizes common cloud computing risks and possible risk responses. While it illustrates common risks and responses, it is not a complete list of all cloud computing risks.

Table 3.2. **Summary of Common Cloud Computing Risks and Risk Responses**

Cloud Computing Risks	Cloud Computing Risk Responses
Reliability and vulnerability	• Vendor due diligence processes • Performance monitoring processes • Security monitoring processes • Incident response processes
Multi-tenancy, data leakage, data theft	• Data classification policies • Data destruction policies • Security processes
Single point of failure	• Data redundancy • Business continuity policies • Incident response processes
Compliance	• External environment monitoring processes • Internal environment monitoring processes • Vendor monitoring processes
Cyber attacks	• Incident management processes
Shadow IT	• Cloud computing policies • Data loss prevention processes • Security monitoring processes

14 Develops Portfolio View

Since cloud computing is part of the overall IT strategy which supports the business strategy, a portfolio view of the risks needs to be developed. This includes assessing public, private, and risks in hybrid cloud models and how the use of different CSP vendors affects the overall cloud strategy which is a part of the overall IT environment supporting the organization. This also involves reviewing cloud computing within business processes to see how its use affects the business units, which can vary. For example, the impact of a risk related to business continuity of an ERP on the Finance department (which may delay reporting or payments) will be very different than on the production floor (which may disrupt manufacturing).

Cyber security risk should be considered when thinking through cloud computing risks. Cyber threats should be looked at holistically with other ERM risks. It is worth noting, the impact of a cyber risk could also be different in different situations, such as, the impact of a cyber breach to a forecasting tool that the Financial Planning and Analysis department uses will be different to a cyber breach to a financial data warehouse that the same department uses. When assessing the portfolio view of cyber security risk, the organization's cloud computing usage should be reviewed against its data classification policies.

As the organization reviews cloud computing risks, they should look at them holistically from different perspectives and departments and across all related cloud systems. These holistic risks should be looked at from strategic, financial, operational, compliance, and reporting objectives point of view and interlaid into the overall ERM risk portfolio.

Table 3.3 **Key Activities for Cloud Computing – Performance Principles**

Principle	Description	Cloud Computing ERM Key Activities
10. Identifies Risk	The organization identifies risk that impacts the performance of strategy and business objectives.	The organization assesses internal and external (including industry, CSP, and the CSP's vendors) environment to identify cloud computing risk.
11. Assesses Severity of Risk	The organization assesses the severity of risk.	The organization considers risk impact and risk likelihood in assessing cloud computing risk throughout the organization.
12. Prioritizes Risks	The organization prioritizes risks as a basis for selecting responses to risks.	The organization prioritizes risks and risk responses to address cloud computing risk.
13. Implements Risk Responses	The organization identifies and selects risk responses.	The organization designs processes and controls to implement risk responses.
14. Develops Portfolio View	The organization develops and evaluates a portfolio view of risk.	The organization views cloud computing risk holistically with risks to strategic, financial, operational, compliance, and reporting objectives.

REVIEW AND REVISION

Table 4.1 **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework* – Review and Revision Principles**[14]

Principle	Description
15. Assesses Substantial Change	The organization identifies and assesses changes that may substantially affect strategy and business objectives.
16. Reviews Risk and Performance	The organization reviews entity performance and considers risk.
17. Pursues Improvement in Enterprise Risk Management	The organization pursues improvement of enterprise risk management.

15 Assesses substantial change

ERM is an ongoing, iterative process. It is not meant to be performed in a vacuum and shelved; likewise, it is not meant to be taken out and updated annually and ignored in between. ERM should be embedded into the way an organization operates.

ERM should be updated whenever there are significant changes to the environment, organization, or CSP, and decisions on implementing and integrating cloud-based services can constitute or prompt substantial changes. Management is accountable for routinely evaluating risks and identifying situations where risk may rise above the organization's risk appetite. In 2020, this included changes caused by the COVID-19 pandemic. Many organizations rushed to facilitate a remote workforce. Often this included an expansion of cloud computing applications to enable employees to interact with technology and operate effectively outside the office. Another substantial change could include additional geographic locations an organization is doing business; the CSPs the organization chooses to work with may need to change in order to provide the appropriate coverage to address latency or address disaster recovery, or they may need additional CSPs to support the efforts.

As noted in the prior section, external changes in the regulatory and compliance environment may also impact cloud computing. and should be monitored. For example, Singapore's amended Personal Data Protection Act will be effective starting February 2021 which includes requirements for data breach notification.

Technology is continually advancing in cloud computing. These advances add additional options for cloud security and migrations which the organization needs to routinely evaluate to see how these may affect business objectives and their ability to create additional value for the organization.

Other substantial internal changes could include mergers, acquisitions, and divestures. Often organizations will have a transition service agreement in a divesture and that could add another layer of complexity to the of managing cloud contracts, access, etc.

Management should be assessing and evaluating its culture as well. As we have seen in the COVID-19 pandemic, remote work has changed the culture for many organizations.

14 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*

16 Reviews Risk and Performance

The cloud computing governance process must be reviewed to identify improvement points. Cloud computing governance process enhancements may include the use of balanced scorecards. The cloud vendors must be assessed against their service level agreements which typically include availability. Cloud contracts should continue to be reviewed before evergreen and auto renewals. Vendors should be audited or System and Organization Controls (SOC) reports should be obtained and reviewed. An organization should also assess changes for its CSPs. Major items such as a breach, even if it did not affect the organization, could impact the organization's ability to achieve its business objectives in the immediate future. Vendor assessments could result in situations that raise risks higher than the organization's risk appetite. In those instances, the organization needs to review the risks and take appropriate action to address the risks. Additionally, controls maintained and performed by the organization should also be reviewed for compliance. Review of control performance could be performed by management, Compliance or by Internal Audit.

The cloud computing and cloud governance processes should be operational with defined roles and embedded into all levels of the organization. Cloud computing governance should not be performed in a bubble; it should be a collective effort across the organization. Risks should be reviewed to ensure the actual residual risk after performance of controls is within risk tolerance levels. Results should be incorporated into the overall ERM process.

17 Pursues Improvement in Enterprise Risk Management

Performance reviews must be taken on the cloud computing process, not just the cloud vendors as part of cloud governance and supplier management. The organization should use the risk and performance reviews to update the cloud governance program, processes, and controls. Additionally, the organization should look at how the cloud governance and cloud processes are feeding into the overall organizational ERM processes. The organization should assess the level of collaboration across departments in the cloud governance program and seek to improve the ERM process with updates. Also, the organization should utilize the output of the ERM process and apply updates and outputs to the cloud governance program.

Table 4.2 **Key Activities for Cloud Computing – Review and Revision Principles**

Principle	Description	Cloud Computing ERM Key Activities
15. Assesses Substantial Change	The organization identifies and assesses changes that may substantially affect strategy and business objectives.	The organization assesses internal and external changes and impact to business strategy and objects as well as the affect they will have on cloud computing strategy or how cloud computing can provide effective infrastructure to realize the changes.
16. Reviews Risk and Performance	The organization reviews entity performance and considers risk.	The organization reviews the cloud governance program. Also, perform cloud governance activities to review CSPs and cloud risks.
17. Pursues Improvement in Enterprise Risk Management	The organization pursues improvement of enterprise risk management.	The organization assesses the cloud program for improvements to be applied to the overall organization ERM program.

INFORMATION, COMMUNICATION, AND REPORTING

Table 5.1 **COSO *Enterprise Risk Management – Integrating with Strategy and Performance Framework* – Information, Communication, and Reporting Principles**[15]

Principle	Description
18. Leverages Information Technology	The organization leverages the entity's information and technology systems to support enterprise risk management.
19. Communicates Risk Information	The organization uses communication channels to support enterprise risk management.
20. Reports on Risk, Culture and Performance	The organization reports on risk, culture and performance at multiple levels and across the entity.

18 Leverages information and technology

An organization should leverage technology to support the ERM function in the identification, communication, response, and management of cloud computing risk. Information to monitor cloud governance could be from a variety of sources including monitoring applications, Internal Audit testing and assessments, vendor management systems, and governance and compliance tools.

In addition to financial rating agencies which may assess an organization's financial health, there are multiple IT security organizations that collect data and can provide a security score on a website, vendor, or CSP. These security ratings provide insight into the security posture of the CSP. There are also organizations that assess reputational risk which can be included in vendor evaluations. These tools along with other cloud monitoring tools to assess the cloud infrastructure and services state (performance, availability, etc.) can be leveraged to manage cloud computing. These external tools should be used to capture new information that could impact the cloud computing governance program.

Some technology may be available from the CSP for the organization to utilize. Other times the CSP may leverage technology tools to gather and share information on the performance of its responsibilities for the organization.

19 Communicates Risk Information

A key component of good governance is clear communication and reporting. Without current information provided to the appropriate individuals, suitable decisions cannot be made. Information should be reported and transparent between all appropriate parts of the cloud computing governance program. Open communication and data sharing ensure all parties are aware of updated impacts to risks and risk responses. It also facilitates a shared and holistic risk management culture within the organization with all departments taking part and being accountable.

As cloud computing is adopted within an organization, the roles and responsibilities for individuals will change. Changes to their responsibilities by application or process should be communicated to the employees. The organization should continue to reinforce its risk aware culture via multiple communication channels. The organization should communicate the cloud governance program is part of the overall ERM program and ensure each employee's role is understood.

The Cloud Computing Steering Committee should be updated on the cloud transition and ongoing cloud computing performance.

15 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*

There should be clear communication avenues between the organization and the CSPs. These will be needed for escalating issues as well as for periodic updates and management of the vendor and relationship.

20 Reports on Risk, Culture and Performance

The board of directors should be updated on the cloud strategy and the impact it is having on business objectives. The organization should also be reporting on cloud computing performance as well as conveying progress on cultural change management and the risk culture throughout the organization. Culture is slow to change within an organization; it takes time. Open and transparent communication helps create the cooperative culture needed within an organization. Reporting should be made available at all levels of the organization so that consistent messaging is provided, and progress and changes are understood throughout.

Different levels of the departments will need to communicate different updates to the board. For instance, the first line, management, should communicate changes to the cloud strategy and business objectives. Compliance, part of the second line, should communicate on CSP monitoring and risks. Internal Audit, as the third line, should report independently and objectively on the organization's cloud computing and activities including communicating issues where risks were not addressed by the first and second lines.

Table 5.2 **Key Activities for Cloud Computing – Information, Communication, and Reporting Principles**

Principle	Description	Cloud Computing ERM Key Activities
18. Leverages Information Technology	The organization leverages the entity's information and technology systems to support enterprise risk management.	The organization utilizes available and implement as appropriate additional platforms to leverage and consolidate cloud computing information and technology data to support enterprise risk management.
19. Communicates Risk Information	The organization uses communication channels to support enterprise risk management.	The organization employs communication channels throughout those involved in cloud computing to support enterprise risk management.
20. Reports on Risk, Culture and Performance	The organization reports on risk, culture and performance at multiple levels and across the entity.	The organization reports on cloud computing risk and performance at multiple levels and across the organization.

CONCLUSION

Cloud computing is one of many technology options available for organizations to utilize. A structured adoption of cloud computing, including a holistic cloud computing governance program that addresses the associated risks and is incorporated into the ERM program, will enable an organization to derive the most value and enable the organization to achieve its strategic objectives.

For an organization to maintain a competitive edge, it will need to use its IT strategy to empower the business. Integrating cloud computing into the IT strategy and turning the IT organization into a strategic partner can provide many of the tools and framework needed for the organization to succeed.

Cloud computing risks must be identified and managed in the context of the organization's broader ERM program. While tasks, processes, and maintenance can be outsourced, accountability for risks cannot. The ownership of the risks will remain with the organization who will need to monitor the internal controls within the organization and of its CSPs.

In order to use cloud securely, organizations should invest and implement a variety of security tools. The organization will need to leverage available technology to continue to monitor, report, and update assessments of the cloud computing technology, vendors, and ERM program. Senior management and the governing body should also ensure that the internal audit activity has included cloud-based services in its risk-based planning process, to provide independent assurance and advice.

Organizations that have already embarked on the path to cloud computing without an ERM framework can and should still add cloud governance to their processes. Since the cloud governance process should be incorporated into the ongoing activities related to business strategy, IT strategy, and cloud computing, the cloud governance should be continually updated and revised based on new information. If an organization has not created a cloud governance program, it can do so at any time and continue to refresh as changes occur. By incorporating cloud governance into the organization's cloud computing processes, the organization is better positioned to manage risks that threaten the strategy and objectives of the organization.

The use of the COSO *Enterprise Risk Management – Integrating with Strategy and Performance framework* enables cloud computing to be integrated with the organization's ERM function. The cloud computing governance approach provides a holistic view of cloud computing throughout the organization. Governance and communication and reporting dovetails with the cloud strategy, performance, and monitoring and revision. This is undertaken with a view that the implementation of cloud computing will coalesce the CSP's cloud computing governance processes with those of the organization.

APPENDIX A.
Roadmap to Cloud Computing

Planning a cloud adoption strategy is a methodical process. This section provides considerations for migrating traditional on-premise workloads to cloud computing. It is focused primarily on IaaS and PaaS.

This roadmap represents an ideal state where governance and strategy are fully contemplated at the beginning of an organization's cloud journey. However, situations and an organization's focus may change and, therefore, the cloud strategy may need to shift as well. Additional cloud computing governance can be added in retroactively and at different stages of the process as a checkpoint to reassess and redirect efforts as needed.

Phased Approach

Highlighted below are the four basic phases of a successful cloud migration journey. Interlaid into the phased cloud migration approach is when to incorporate the COSO ERM framework components.

At beginning of the cloud migration, prior to the detailed assessment of the IT environment, the organization should define the cloud **governance and culture**. A Cloud Computing Steering Committee can provide oversight and structure the responsibility matrix. Once the oversight structure is established, the organization can work to define its cloud strategy in relation to the organization's overall mission and strategic objectives during the ERM **strategy and objective-setting**.

Assess

During this phase, organizations assess their IT portfolio where infrastructure discovery and application rationalization is performed. While assessing infrastructure discovery, 'as-is' infrastructure landscape is analyzed and details such as server configuration, utilization parameters, network segmentation, storage allocation, and dependencies are collected.

During the application rationalization process, applications are grouped depending on the factors such as application complexity, criticality (including future business trends), and dependencies. Each application is assigned a migration path to follow during migration phase. Total cost of ownership (TCO) analysis is performed wherein 'as-is' spend is compared against 'to-be' spend in the cloud. Typically, at this stage, organizations identify teams to successfully execute the cloud roadmap and prepare a migration plan. Usually, the cloud offers cost savings due to only paying for storage and computing power based on usage and by shifting costs to operating expenses (over capitalized expenses).

As the migration path is defined, this is a good point to review the cloud performance using the ERM **performance** component in the framework. Risks to the cloud should be identified and mitigation steps put in place.

Build

During this phase, organizations can build a foundation to host a cloud environment that accounts for scale, security, governance, networking, and identity. It is called the landing zone. A poorly planned foundation can cause organizations to face delays, confusion and downtime, and jeopardize the success of the cloud migration. The objective of setting up a cloud landing zone is to build the foundation to develop, test, deploy, monitor, and maintain. Governance, management and subscriptions are established while defining the landing zone. Network, compute, storage, database, management, monitoring, security, continuous integration and continuous development (CICD), application migration, and analytics capabilities are established. Activities are assigned to resources to drive transformation, establish governance, create a cloud center of excellence, define security at all levels, fulfill compliance, design policies, define architecture, and detail plans for transformation (people, process and technology).

Migrate

During this phase, applications and workloads are migrated to the cloud landing zone as per the migration path defined during the assessment phase. Depending on how large an application portfolio an organization has, cloud migration is an iterative process to migration workloads. These iterations are essentially different waves or move groups based on the dependency matrix and business priority defined in the migration plan during the assessment phase.

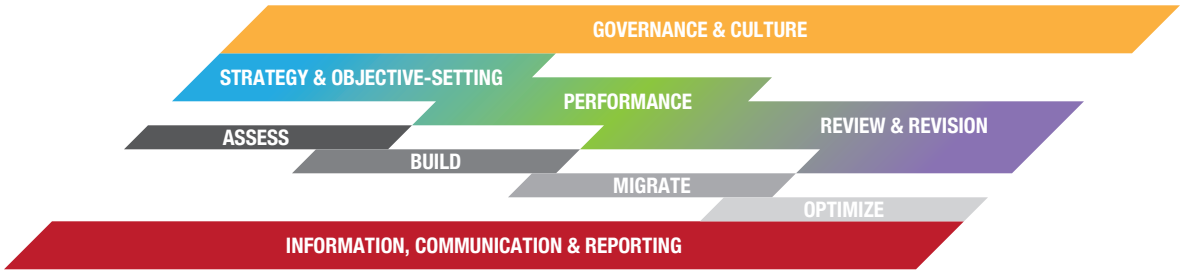
As the cloud is setup and expanded, the cloud governance should be **continually reviewed and revised** to assess changes to the environment or organization.

Optimize

Depending on how mature the organization is, the landing zone setup to establish the foundation of the cloud environment can be started small and then expanded. Mature organizations usually start with enterprise scale. During the optimization phase, the cloud environment is refined to make it more efficient. It is an ongoing and continuous process as the environment evolves.

Once the cloud is operational the organization should leverage the cloud for ERM **information, communication, and reporting**. This will allow the organization to report on the cloud and CSP.

Diagram 10. **The Roadmap to the Cloud should include the COSO ERM Framework**



Tactical Migration Strategies

There are six different migration paths available to migrate workloads to the cloud, each carrying its own risks. This is also called the 6 R methodology. These migration paths are assigned during the assessment phase of the cloud migration. The cloud migration is carried out primarily through adoption of one of the "R" approaches mentioned below.

Retain

This approach tends to be applicable to a hybrid IT environment in which the organization is not ready to move their entire workload to the cloud. This is typically a temporary approach to "retain" some of the on-premise workloads until the organization is prepared for a full transition. Cloud transitions can be an extended project and may include some temporary (or permanent) retention of on-premise services.

Rehost

This is the easiest approach for cloud migration. This approach would entail the organization's current servers and workloads be translated to the desired cloud environment without the need for any changes to the software or platform. For many migrations, some workloads can simply be rehosted while others will require a more involved approach. This is frequently referred to as lift and shift.

Replatform

Some workloads may require changes to the platform it runs on. This might entail changing the operating system the software runs on or transferring the data to a new database engine. While some workloads may translate directly to a cloud platform, others may require replatforming.

Repurchase

This approach represents the option to switch products entirely, typically to a SaaS application. This approach is usually followed for third party products which have been running on-premise and their licenses cannot be ported in the cloud version of the same product e.g., commercial off-the-shelf (COTS) applications.

Refactor

Workloads will often require architectural changes to fully leverage cloud native services. Refactoring might include changing the organization's solutions by rebuilding software to be containerized so the organization can utilize cloud resources at their maximum efficiency. Older monolithic software solutions might not translate well to the cloud and could benefit from refactoring. Refactoring software may entail some level of replatforming the final solution as well.

Retire

This approach is followed for the assets and applications which are identified to be decommissioned in the migration plan during the assessment phase of the cloud migration. This might entail workloads that have already successfully been transitioned to the cloud, or possibly a solution that is no longer necessary in a cloud environment.

In the table below, we highlight the risks and benefits of the primary migration approaches.

Table 6.1. **Tactical Cloud Migration Approach Risks and Benefits**

Approach	Benefits	Risks
Rehost	• Higher speed of migration • Reduced risk of migration • CSP + partner ecosystem of tools to natively support this migration approach • It could be automated/tool assisted	• May not use PaaS services • Inherit potentially same performance characteristics • Limited retirement of technical debt
Replatform	• Uses cloud services with no code change required • No dependency on underlying physical hardware platform • Migration to newer platform • Opportunity to modernize technology stack • Automated tool assistance available in some cases	• Migration could be time consuming and costlier • Requires additional planning and coordination
Repurchase	• Eliminates dependency on custom hardware or proprietary technology platforms • Could be direct adoption of SaaS solution eliminating the overhead of maintaining application and infrastructure	• Careful evaluation of partners/vendors needed • Some use cases can grow in time and effort • Data migration is required
Refactor	• Utilizes cloud native features • Increases efficiency and agility at improved cost • Adapts to modern customer needs • Eliminates dependency on customer hardware and proprietary technology platforms • Improves user experience	• It could be complicated, expensive and could impact migration timeline. • It requires a good understanding of all aspects of the application, compliance, regulatory requirements, security, code, design etc. • Some use cases can go grow in time and effort

APPENDIX B.
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.

Depending on the size and complexity of the organization, some of these positions may not have a direct match; therefore, please use these as a guide and align or combine to appropriate individuals within the organization. Additionally, to the extent possible, organizations should align the cloud governance responsibilities with existing ERM responsibilities.

Table 7.1. **Roles and Responsibilities in the Cloud**

Position	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 • Participate in the ERM process
Chief Executive Officer	• Define the organization's business strategy and how cloud computing enables it • 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 • Participate in the ERM process
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 and internal IT services • 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 CSP • Participate in the cloud governance process • Participate in the ERM process
Chief Legal Officer	• Ensure that the organization's cloud activities comply with laws and regulations • Monitor for changes in the organization that could result in additional compliance needs • Monitor for new laws and regulations that would impact the organization's cloud solution or its CSPs • Review and approve cloud service 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 • Participate in the cloud governance process • Participate in the ERM process

Table 7.1. **Roles and Responsibilities in the Cloud**

Position	Position Responsibilities
Chief Risk Officer	• Manage the organization's overall ERM efforts including the incorporation of cloud computing • Monitor changes to the organization and the overall environment • Coordinate with the Chief Compliance Officer on CSP compliance • Monitor and assess changes to culture
Chief Compliance Officer	• Monitor for changes in the organization that could result in additional compliance needs • Establish a plan for compliance for new regulations that impact cloud activities • Monitor the organization's cloud activities against compliance requirements • Participate in external reviews, such as for SOC 2, PCI-DSS or regulatory compliance • Monitor CSPs for applicable compliance • Participate in the cloud governance process • Participate in the ERM process
Chief Information Officer or Chief Technology 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 for new products and services • Facilitate the integration of cloud solutions into operations and the organization and current IT infrastructure • Enable the change and the success of the organization in the cloud • 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 internal cloud incident management program • Establish processes and protocols with CSPs for incident management • Participate in the ERM process
Chief Information Security Officer	• Establish strategy and oversight to secure information and technology assets in the cloud • Enable the change and the success of the organization in the cloud • Perform cyber security assessments, such as penetration assessments or review the results from cloud vendors • Ensure adequate security controls are established for cloud-based services • Monitor cloud-based services for indicators of cyber-attacks or internal misuse of resources • Participate in the cloud governance process • Participate in the ERM process
Chief Audit Executive	• Perform risk-based 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, PCI-DSS, or other regulatory compliance 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 • Participate in the cloud governance process • Participate in the ERM process
Privacy Officer	• Maintain the organization's privacy program • Review the data classification policies and what data may migrate to the cloud • Monitor how CSPs comply with the organization's privacy requirements • Participate in the ERM process
Cloud Computing Steering Committee	• Provide oversight over the cloud migration process • Monitor the organization to ensure overall cloud governance is incorporated into processes • Participate in the ERM process

Table 7.1. **Roles and Responsibilities in the Cloud**

Position	Position Responsibilities
Strategic Sourcing or Procurement	• Coordinate with business process owners to define requirements for cloud computing vendors • Maintain an approved list of cloud vendors • Evaluate potential CSPs for fit • Participate in the ERM process
Vendor Risk Management	• Define vendor management policies for CSPs • Monitor CSP service-level agreements • Monitor activities of the CSP and fellow cloud tenant customers • Participate in the ERM process
Technology Architect	• Design the overall technology strategy for the organization including the cloud strategy and environment, including systems and software • Implement and maintain the overall IT environment
Network Engineer	• Design and implement network architecture to enable the availability of the systems and applications in and out of the cloud • Maintain cloud infrastructure (IaaS and PaaS) • Optimize network software • Implement and maintain communication and hardware connections in and out of the cloud
Security Engineer	• Design strategy and implement tools to protect the security, confidentiality, integrity, and privacy of the cloud environment • Monitor the cloud environment for potential threats • Manage incident response for the organization • Liaise with the CSP for incident response
DevOps Engineer	• Maintain processes for development and operations for the cloud • Create functional, scalable, fault tolerant applications for the cloud
QA Engineer	• Test systems and application changes for the cloud • Prepare data for business continuity planning for the cloud
System/ Application Administrator	• Maintain application user administration and security for the cloud systems and applications • Manage system configuration • Monitor managed services for cloud processes • Manage maintenance for cloud systems, as necessary
CSP Relationship Managers	• Note, there will be multiple, based on different departments • Maintain relationship and contacts with CSPs • Escalate incidents with CSP when necessary • Monitor and enforce CSP service-level agreements
End Users	• Safe and appropriate usage of cloud applications and tools • Understanding of data privacy and security practices

APPENDIX C.
Glossary and Definitions

The introduction provided three definitions of cloud computing. Again, in the simplest terms, cloud computing is a computing model that utilizes pooled resources over the internet. The management of the underlying servers and processes may be outsourced to another organization. The following outlines some key cloud terms used throughout this paper.

Cloud Computing Terminology

Common cloud computing terminology is explained below:

- **Cloud Service Provider (CSP)** – A vendor that provides cloud computing services that could include infrastructure, networking, or business applications.
- **Managed System Provider (MSP)** – A vendor that manages an organization's IT needs. A CSP is an MSP, but an MSP does not have to be a CSP, an MSP could manage non cloud processes as well.
- **Managed Cloud Services** – The managed services provided by the organization's CSP. These will vary based on the delivery method and the contract.
- **Multi-cloud** – An organization that utilizes multiple deployment models, delivery models, and/or different platforms with different public cloud service providers is in a multi-cloud environment. Multi-cloud can be a strategic decision; although, it can arise from uncoordinated efforts by different departments.
- **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 Access Security Broker (CASB)** – a security application that resides between cloud users and cloud applications to apply the organization's security policies to the cloud resources. CASBs are used to protect data and enforce security policies.
- **Secure Access Service Edge (SASE)** – applies cloud-based policy and delivers secure cloud access. SASE focuses on networking and security.
- **Containerization** – is a method to manage workloads and services which facilitates automation.

Cloud Deployment Models

The most common cloud computing deployment models include:

- **Private cloud** – A private cloud is created only for one organization and managed by the organization or a CSP.
- **Community/Partner cloud** – A community or partner cloud is shared by organizations with common interests (e.g., mission, industry collaboration). It might be managed by the community organizations or a CSP.
- **Public cloud** – A public cloud is managed by a CSP who makes the services available to people or organizations who want to use or purchase them.
- **Hybrid cloud** – A hybrid cloud is composed of two or more clouds (private, community, or public) environments that must include a private cloud and remain unique entities with communication between each cloud entity. Hybrid clouds are used to provide flexibility on workloads.
- **Government cloud** – A government cloud is designed for government organizations or institutions to meet government requirements on security. These may be managed by a government or by a CSP.

Cloud Service Delivery Models

The most common cloud computing delivery models include:

- **Infrastructure as a Service (IaaS)** – The CSP provides an entire virtual data center of resources (e.g., computing resources, and storage resources).
- **Platform as a Service (PaaS)** – The CSP provides proprietary tools that facilitate the creation of application systems and programs that operate on the CSP's hosted infrastructure.
- **Software as a Service (SaaS)** – The CSP provides a business application that organizations can use to perform specific functions or processes (e.g., email, customer management systems, enterprise resource planning systems).

Pricing Models

The most common cloud computing pricing models include:

- **Subscription** – Paying a fee typically based on licenses or seats. This is frequently used for SaaS and is usually set at monthly interval.
- **Usage** – Based on usage, which may include storage used, computational power, time, bandwidth, backup, and/or support.
- **Tiered** – Fee levels based on usage or features. This could be tied to a subscription-based or usage-based model.
- **Combined** – A pricing model that may take aspects of pay as you go, tiered, and/or subscription.
- **Dynamic** – A pricing model that adjusts based on supply and demand. Users can pay the current demand price, or they can pay a reserved price and obtain resources at a set time.
- **Market** – Pricing can differ if the organization uses on-demand time vs setting a price limit. Pricing changes are based on supply and demand at the time of service. If the organization set a price limit, like a reverse auction, and the price goes down to the organization's price, the organization's workload will be executed.
- **Advertisement** – Pricing is typically either low or free, but the user is subject to advertising to use the system.

ABOUT THE AUTHORS

Mike Grob, Principal, Crowe LLP

Mike Grob is a Principal in Crowe LLP's Consulting Practice. In this role, he leads cloud transformation services and assists clients in modernizing their IT services. He is a Microsoft Certified Professional in Azure and Dynamics.

Mike has a BS in Media and Communications Strategy from Michigan State University.

Victoria Cheng, Managing Director, Crowe LLP

Vicky is a Managing Director in the Consulting Practice at Crowe LLP. She focuses on IT risk management and cloud governance.

Vicky graduated from the University of Illinois. Vicky is a CPA licensed in Illinois and a CISA. She is a member of AICPA, ICPAS, IIA, and ISACA.

ABOUT COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

ABOUT CROWE

Crowe LLP is a public accounting, consulting, and technology firm with offices around the world. Connecting deep industry and specialized knowledge with innovative technology, our dedicated professionals create value for our clients with integrity and objectivity. By listening to our clients, we learn about their businesses and the unique challenges they face. We forge each relationship with the intention of delivering exceptional client service while upholding our core values and strong professional standards. We invest in tomorrow because we know smart decisions build lasting value for our clients, people, and profession.

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

ENTERPRISE RISK MANAGEMENT FOR CLOUD COMPUTING

COSO

Committee of Sponsoring Organizations of the Treadway Commission

coso.org