A REPEATABLE CLOUD-FIRST DEPLOYMENT PROCESS MODEL
ACKNOWLEDGEMENTS

AUTHORS
Lorraine Barnes
Luciano Santos
Ryan Bergsma

CONTRIBUTORS
Vincent Campitelli II
Matt Keil
John Yoeh Daniele
Daniele Catteddu
# TABLE OF CONTENTS

## INTRODUCTION 4

## PLAN 6
- Identify the business drivers 6
- Determine the stakeholders 6
  - Stakeholder roles 7
  - Qualification assurance 8
- Assess the organization’s assets 8
  - Review the existing architecture and services 8
  - Data classification 9
- Select your service and deployment model 9
- Identify existing business controls 10
  - Consult the governance model 12
  - Security and compliance 12
  - Contractual obligations 12
  - Risk 12
- Design for the new environment 13
- Assess the Cloud Service Providers’ Controls 14
- Identify control gaps 15
- Verify solutions to fill control gaps 15

## DO 16
- Select a Cloud Service Provider 16
- Negotiate SLAs 16
- Build as Required 17
- Implement controls to fill the gaps 17
- Launch 17

## CHECK 18
- Monitor 18
- Account 18

## ACT 19
- Respond to any Incidents 19

## CONCLUSION 20
The term “Cloud First” was initially popularized by Vivek Kundra, who formerly held the post of White House CIO and launched this strategy for U.S. federal government IT modernization at the Cloud Security Alliance Summit 2011. The underlying philosophy of the cloud-first strategy is that organizations must initially evaluate the suitability of cloud computing to address emergent business requirements before other alternatives are considered.

For many organizations, the cloud-first strategy begins an elaborate and sometimes complex series of business and technology decisions. Understanding and weighing all the software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure as a service (IaaS) options that are available is a monumental task, and it can be hard to know where to begin the process of creating and implementing a cloud-first strategy.

By now the benefits of cloud computing are generally understood at high level. What is not necessarily clear are the details of the potential security, legal, financial, and compliance impacts that cloud adoption will produce. The stakeholders who are currently responsible for these areas are sometimes not sufficiently familiar with how a cloud-first strategy affects their roles and functions. While the organization as whole is still responsible for ensuring that all its obligations are met, the cloud changes the nature of risks, roles, and responsibilities and how stakeholders within the organization manage them.

Cloud computing is a shared responsibilities model, where different entities are responsible for managing their areas of concern across the entire implementation as appropriate for the specific SaaS, PaaS, or IaaS model that is chosen. Successful cloud initiatives must have top-down support, but just as critically, they need to be viewed as a collaborative effort due to the breadth of subject matter expertise that is required from all parts of the business.

There are compelling reasons to establish a process that engages all the right stakeholders at the right times. An article by Continuity Central which references a 2014 survey by CSA states that “54 percent of IT and security professionals said they have 10 or fewer cloud-based applications running in their organization, with 87 percent indicating that they had 50 or fewer applications running in the cloud (with a weighted average of 23 apps per organization). These estimates are far lower than commonly reported by vendors and research reports, which count more than 500 cloud apps present, on average, per enterprise.” In other words, cloud computing deployment is often happening without IT knowledge or authorization—and even more likely without the company's security, procurement, legal, compliance, and other relevant teams being consulted. Because these deployments occur outside the context of a well-defined cloud strategy, companies end up exposing themselves to the very risks that the specific teams are tasked with managing for the business.

It’s important to recognize that cloud-first isn’t an initiative that has an end date. In fact, whether the organization decides to move most or all of its infrastructure to the cloud or it starts with just a few SaaS applications, cloud-first is just the beginning of an ongoing process of assessments and decisions that an organization will need to make if it wants to continue to ensure that its best interests are protected.

This paper offers guidance to help organizations establish a systematic and repeatable process for implementing a cloud-first strategy. It offers a high-level framework for identifying the right stakeholders and engaging with them at the right time to reduce the risk, liabilities, and inefficiencies that organizations can experience as a result of ad-hoc cloud decisions. The goal of this guidance is to help ensure that any new cloud program is secure, compliant, efficient, and successfully implements the organization's key business initiatives.
A CLOUD-FIRST MODEL

PLAN

ACT

CHECK

DO

©2016 Cloud Security Alliance | All Rights Reserved.
IDENTIFY THE BUSINESS DRIVERS

The first step is to identify the specific business problems that need to be addressed. The organization’s cloud champion—the person who is mandating or authorizing a cloud-first strategy—will play a large role in specifying the business motivations and expectations behind the cloud-first directive. The organization will then look at specific requests from individual business groups through the cloud-first lens. Whether it’s a small ask, such as a request for an HR application, or a larger initiative, such as IT looking to supply computing power in a more scalable and agile way, it will be important to identify specific and measurable goals for each project. It may seem obvious, but without clearly recognizing and prioritizing the business drivers upfront, it will be difficult to develop a cohesive plan and evaluate its success. The further into the process the organization gets, the more chances there will be to become distracted by the sheer quantity and versatility of all the SaaS, PaaS, and IaaS options and deployment models that are available. In many cases, it can be helpful to start with a small project that offers a quick return, from which the organization can then build on further success. It is important to remember that regardless of the scope of the project, documenting the desired business outcomes—and how results will be measured—will serve as a compass to ensure that the cloud strategy stays aligned with the organization’s key business objectives.

DETERMINE THE STAKEHOLDERS

Gathering the right people together to embark on this collaborative effort is perhaps the most important aspect of creating and implementing a successful cloud-first strategy. Cloud service providers will make claims and offer assurances in terms of security, compliance, SLAs, and other issues that are of vital importance to the business. But even when certain responsibilities are shifted to the cloud service provider—which will vary according to the SaaS, PaaS, or IaaS model that is chosen—it is still the organization that will ultimately bear the consequences of any failures to meet its commitments. As services move to the cloud, subject matter experts across the organization will need to become educated on how these moves may change risk and the business’s ability to meet its obligations. They will need to perform due diligence in evaluating whether or not the potential cloud service providers can support the organization’s requirements, communicate those findings and potential business impacts throughout the process, and provide ongoing oversight over those areas to ensure that needs continue to be met.
The essential stakeholder roles that will need to be engaged are outlined below. It should be noted that these roles are assigned and combined in countless ways in different organizations. Smaller organizations should keep in mind that some of these roles (legal, for example) may be outsourced. When that is the case, an internal stakeholder will need to be responsible for managing that engagement. In whatever ways the various stakeholder functions are distributed within an organization, what is most important is to ensure that all functions are accounted for and the owners of specific responsibilities are documented.

**Stakeholder roles**

**Cloud Champion:** As the person who is mandating a cloud-first strategy—often the CEO, CIO, or CSO—he or she will be important to establishing what the business drivers are for implementing a cloud strategy.

**Cloud Lead:** Most likely the person who is using this guidance document, he or she is tasked with managing the cloud decision-making process. This person will need to help educate other stakeholders on how their roles may change as the organization moves to the cloud and will coordinate those roles.

**Cloud Strategist:** If the organization does not already have experience in cloud adoption, it will be important to consult or hire a person with the necessary expertise. A cloud strategist will have a thorough understanding of current cloud technologies and be able to help map the organization's business problems to appropriate offerings in the most efficient and strategic ways.

**Legal:** In the cloud, the contract with the cloud service provider is the only way to guarantee coverage of responsibilities, so the stakeholder representing the organization's legal interests must play a strong advisory role right from the start. He or she will communicate the relevant laws and contractual obligations, convey the consequences of failing to meet those standards, and help negotiate contracts. This role will also need to ensure that the workforce is educated on appropriate behaviors with regard to security and the use of cloud services.

**Governance, Risk, and Compliance (GRC):** GRC stakeholders will manage all areas of the organization's potential exposure, ensure compliance with the relevant laws and regulations, and ensure appropriate governance of internal business controls. This includes validating cyber-security insurance coverage, disaster recovery and crisis management plans, and data privacy and data loss protection. Owners of individual compliance requirements—such as PCI, GLBA, HIPAA, and other data privacy standards—will be responsible for communicating the details of compliance requirements and necessary controls.

**Finance:** If there are financial goals driving the initiative, finance will need to determine the means by which results will be measured and provide ongoing analysis. Cloud adoption will likely shift costs away from capital expense toward subscription-based costs, so finance will need to adjust financial planning and analysis as well as financial reporting and investment analysis. The organization's costing and reporting models will also need to adapt to complex pricing and billing arrangements.

**Vendor Management & Procurement:** This stakeholder’s functions include performing due diligence to evaluate cloud vendors’ financial viability, negotiating for the best pricing and terms, and mitigating risks to protect the organization with regard to data security, SLAs, and exit rights in the event that a cloud service provider is terminated. This is most likely the role that has primary responsibility for ongoing management of the vendor relationship.

**Information Security:** This role will need to become very knowledgeable about cloud security and understand how to work with the cloud service provider to determine exactly where responsibility lies for all aspects of data protection,
disaster recovery, crisis management, and other security matters, ensuring that the company can meet its legal and GRC obligations through both policy and technical means. For SaaS deployments, the security stakeholder will need to have the expertise to verify the cloud service provider’s security controls. In PaaS and IaaS deployments, security will need to be able to contribute to the secure design of the new environment.

**Information Technology (IT):** This set of stakeholders will need to understand how the cloud redefines their roles. In SaaS deployments, their responsibilities will become less about implementation and more about performing due diligence, helping to ensure that cloud contracts meet business requirements, and collaborating with the cloud service provider to provide oversight and expertise to ensure that business requirements continue to be met. With PaaS and IaaS, the change in responsibilities may be more about developing new skills to be proficient in the new environment. Critical IT functions include:

- **Engineering:** The job of designing the enterprise architecture will change considerably if the organization is moving from a mostly on-premises environment, and different SaaS, PaaS, and IaaS will have different impacts on the architecture. Engineering will need to gain a thorough understanding of cloud technologies and infrastructure to be able to help design, integrate, and validate new architectures.
- **Network Administration:** While this role will still be responsible for helping to keep the enterprise up and running, the focus will shift to understanding how cloud security controls affect ongoing operations and working with the cloud service provider to clearly document which functions are the responsibility of the cloud service provider and which remain with the organization. This role will also need to communicate any new cloud policies to end users.
- **DevOps & Software Development:** As internal and external applications move to the cloud, these stakeholders will need to understand how coding practices, application architecture, and the development process will need to evolve. This includes addressing security concerns that may be introduced and the impact of the necessary cloud security controls on development practices.
- **Business Groups:** Individual groups will articulate the business needs that initiate consideration of cloud solutions. These groups may come from any area within the organization, including stakeholders listed above.

**Qualification assurance**

In selecting stakeholders to participate in the cloud-first initiative, it will be important to assess the qualifications and skills that are needed to successfully fill the required roles. In many cases, the organization may lack existing employees with the experience, training, and certifications to perform certain functions. The change in core competencies may require an investment in training or hiring to acquire the necessary skill sets.

**ASSESS THE ORGANIZATION’S ASSETS**

**Review the existing architecture and services**

The IT and security stakeholders should document the existing IT and security service architecture to ensure it is well-understood and to limit complications during
implementation of the cloud strategy. This includes performing a cloud discovery exercise. Even when there has not been a conscious, organizational directive to move to the cloud, it is common that some segment/s of an organization will already be using cloud services in some capacity. The business needs and motivations behind those implementations must be integrated into the overall migration strategy.

**Data classification**

In consultation with legal and relevant business group/s, GRC will take the lead in classifying data to determine the level of confidentiality and protection that is required based on compliance and risk, intellectual property and other concerns. The ultimate goal of these efforts is to determine which data should and should not be permitted in a public cloud environment.

In most cases, it is best to start this process by classifying data into three to five, high-level types. Keep these high-level categories as simple and straightforward as possible. Once these classifications are established, it may be necessary to create subcategories for further clarity. One of the biggest factors that should inform data classification is a recognition of any regulations that may apply to the data. Regulations may originate internally and/or externally.

Other considerations for data classification may include (but are not limited to):

- Data residency
- Personal Health Information (PHI)
- Personal Identity Information (PII)
- Payment Card Industry (PCI)
- Intellectual Property (IP)
- Classified material

It is also important to consider if your data sets can be correlated in some manner to create regulated data, although various data on its own may not have regulated properties. The regulation threshold is often crossed when two or more data sets are combined.

**SELECT YOUR SERVICE AND DEPLOYMENT MODEL**

The decision of which service and deployment models to implement will depend on factors that are unique to every organization. The cloud lead will be responsible for organizing the team and facilitating discussions regarding these selections. Depending on the size of the organization and level of executive involvement in the process, the cloud champion will approve the final service and deployment models and validate that they align with the established organizational goals.

Based on the [The NIST Definition of Cloud Computing](https://www.nist.gov/itl/cloud-computing), service models include:*  
- **SaaS**: The cloud service provider gives the organization application access through a client interface. The cloud service provider controls and manages all of the underlying infrastructure as well as the applications.
• **PaaS:** The organization creates and deploys applications onto the cloud service provider’s platform using the cloud service provider’s programming tools and services. The cloud service provider controls the underlying infrastructure and operating system, but does not manage the applications.

• **IaaS:** The organization deploys applications using programming tools and operating systems of its choice. The cloud service provider controls the underlying infrastructure but the organization manages the applications and operating systems. Furthermore, the organization can provision processing, storage, networks and other computing resources.

Deployment models include:

  • **Public:** Use of the infrastructure is shared among the cloud service provider’s customers and exists entirely on the cloud service provider’s premises.

  • **Community:** The infrastructure is provisioned for exclusive use by a specific set of organizations that have shared concerns (e.g., mission, security or compliance requirements). It may exist on or off premises and be owned and operated by one or more members of the community or a third party.

  • **Private:** The infrastructure is provisioned for exclusive use by one organization and may exist on the organization’s premises or elsewhere. It is often owned and managed by the organization itself but may be operated by a third party.

  • **Hybrid:** The cloud infrastructure is comprised of two or more different deployment models with portability of data and applications between the different infrastructures.

**Factors in choosing a model**

The choice of which models to use will predominantly be driven by a clear identification of business drivers and an assessment of an organization’s required controls with respect to relevant data, applications and services. These factors will likely direct the organization to a particular service and/or deployment model.

• **Data:** It is important to know where data will reside with a given service or deployment model, and the following questions should be considered.
  - What is the classification for any data involved in a new implementation and what governances exist for that type of data that would restrict its location?
  - Who is responsible for ensuring encryption of data when it is in motion or at rest?
  - What type of encryption will be used?
  - Should data reside on a system that does not have network connectivity?
  - Is data required to remain on-premises?
  - Can data cross international borders?

• **Applications:** The selection of appropriate cloud applications is an involved process that should include thorough organizational self-evaluation. Questioning is critical.
  - Does the needed application already exist as an SaaS offering? If it does, are employees already using it without the knowledge of the IT department?

Additional questions should touch on the following topics:

  - **Build versus. buy:** What are the costs of building what is needed versus buying it from a cloud service provider? How do scalability, availability, features, licensing, and portability factor into the decision? Does the organization have the ability to deploy internal software as a service to a
- **Greenfield versus Brownfield:** What are the costs and benefits of starting from scratch in the cloud versus trying to move existing services to a cloud model or supporting legacy? Does the organization currently have the developer skillset for support and migration with new methodologies and technologies (e.g. DevOps, containers, etc.)?
  - **Greenfield considerations**
    - Is there a team that understand the methods used for developing in the cloud?
    - Will the team be implementing a SecDevOps model?
  - **Brownfield considerations**
    - Are skilled legacy coders available? How long will they be available?
    - What are the costs of supporting and maintaining legacy code?
    - How will the codebase perform in a cloud environment?
    - Does your organization have access to professionals with expertise in how to migrate? Is it even possible to migrate?
- **Lift and shift:** The concept of “lift and shift” is the extreme of the Brownfield model where an attempt is made to move an application as a whole to the cloud with no changes. In most cases, this model should be avoided, as it will not make use of many of the tremendous advantages of current cloud technologies. Furthermore, it is likely to be fraught with many difficulties.
  - **Infrastructure:**
    - **Hybrid potential:** Can the cloud model work with on-premises data and applications in the cloud, or on-premises applications and data in the cloud? Or perhaps the application can be a private cloud SaaS offering and the data can reside in a public cloud space?
    - **Cost:** What is the cost difference, over time, for maintaining physical infrastructure versus the cost of IaaS?
    - **Audit trail:** What model will provide the needed audit trail capabilities for data that resides on the company’s infrastructure?

Considerations that apply to all deployment or service models include:
  - **Exit strategies:** Can the organization revert or move to another model if the selected model fails?
  - **Performance differences:** The agility, flexibility and elasticity of each model being explored should be taken into consideration.
  - **Business needs:** Whatever service the business unit has requested, communication should be established and maintained between relevant parties regarding possible model options. The business units need to understand the potential benefits and possible pitfalls of the various models being considered.

Once the service and deployment models have been selected, vendor management will need to validate them against what is available from cloud service providers. In some cases, it may not be possible or it may be prohibitive to move legacy systems to a cloud environment.
IDENTIFY EXISTING BUSINESS CONTROLS

Keeping the key business objectives in sharp focus, the cloud lead will organize the stakeholders to document a complete set of the security, compliance, legal, contractual, financial, and other business requirements that are relevant to the specific initiative. Providing effective guidance may require the cloud lead to educate stakeholders on their changing roles and ensure that they understand and meet their responsibilities. The cloud lead will need to recognize interrelated and conflicting needs and reach resolution on a cohesive set of requirements.

Consult the governance model

If there are current decision-making processes in place, the organization will need to assess how decisions about moving to the cloud will fit within the current framework, and in what ways roles and processes will need to change. At its core, the governance model needs to describe:

- Who makes the decisions?
- How are the decisions made?
- How does the business evaluate the results of decisions over time?

Again, every organization is different, so documenting a governance model that aligns management and oversight with the specific organizational structure and culture will be key to ensuring that the cloud initiative is able to move forward and maintain momentum.

Security and compliance

Legal will need to identify the relevant laws and regulations related to security and compliance in all applicable industries and locations. Stakeholders responsible for specific compliance requirements will need to specify the business controls that are necessary to meet the requirements, and verify whether cloud service providers under consideration have the correct certifications and can meet the organization's compliance needs. Security and engineering will need to provide input on the security controls that are necessary to protect data and information assets.

Contractual obligations

Legal will also need to surface the organization’s contractual obligations with regard to SLAs, data protection, privacy, etc., and ensure coverage of special issues such as electronic discovery obligations and jurisdictional requirements. Vendor management will begin assessing cloud service providers’ abilities to address security concerns, performance and uptime expectations, insurance coverages, and other requirements related to the organization’s SLAs.

Risk

Whether identifying security risks specific to operating in the cloud or communicating the appropriate insurance requirements, risk management will need to conduct due diligence and surface information about all potential areas of cloud-related risk. This includes consideration of integration and connectivity issues that may arise when one cloud service is dependent on another cloud service.
DESIGN FOR THE NEW ENVIRONMENT

While there may be an inclination to assign this step to the IT stakeholders and focus on the technical aspects of design, it is important for the cloud lead to keep the relevant business group/s and the rest of the team engaged. This will ensure that design decisions are not made in a vacuum so that they do not create avoidable problems or limit the business in the future.

- **SaaS:** For SaaS deployments, the organization may have little to no input on design, but there may still be important considerations such as identity and access management. If the organization does not already have a federated identity and access management solution in place, this is another piece of the cloud initiative that will need to happen.

- **PaaS:** If PaaS is being implemented, the software development and DevOps stakeholders will need to consider the impact the new environment will have on development processes. If the organization has not already adopted a DevOps model of continuous integration, development processes will likely need to undergo significant changes. The move to PaaS may also involve additional costs for new tools and training.

- **IaaS:** In an IaaS deployment, engineering will have primary responsibility for defining the architecture and will proactively collaborate with the cloud service provider and vendor management to verify that the design aligns with the contract, delivers the desired benefits, and meets the organization’s requirements now and in the future. Network administration will ensure that the architecture will continue to support end users’ working requirements and that there is no disruption or loss of productivity.

For any type of deployment, security will need to validate that best practices for cloud security are being followed. This is a critical stage for the future of the cloud implementation, especially in an IaaS deployment. It is where the organization has its best opportunity to avoid future complexities and expenses by ensuring that security measures are built into the design rather than bolted on later. DevOps and software development will work with security and compliance to ensure adherence to the appropriate secure coding practices and necessary controls.

Governance should assess if designs include the necessary internal business controls and provide the most efficient way to meet business needs. In IaaS deployments, this is a good time to note that the traditional need to overprovision physical architecture is no longer necessary in a cloud environment due to the elasticity of cloud services.

Legal and compliance should be consulted to ensure that designs align with SLA and compliance requirements. Risk management will need to surface any risk exposure that the design options present and work with cloud service providers to ensure that appropriate incident response plans are developed to address identified risks.

Extending the cost/benefit analysis from the previous step, finance will tighten up the figures used based on the specific design choices that are made.
ASSESS THE CLOUD SERVICE PROVIDERS’ CONTROLS

This is an important phase where the organization takes responsibility for verifying that all controls that the business requires are covered. Security will work with the cloud service providers under consideration to validate that all security controls are appropriate and correctly implemented. Validation should not rely solely on the information from the cloud service providers but also on independent verification, such as the resources available in the Cloud Security Alliance Security, Trust & Assurance Registry (STAR) program. Because registrations and certifications can change fast, cloud service providers may need to provide updated information on upcoming certifications.

It is very important that there is clear identification of which security controls are the responsibility of the cloud service providers and which are the responsibility of the organization. The cloud lead and/or vendor management may help document these responsibilities.

Governance, risk, and compliance should verify that all of the stated requirements are covered by the security controls. At this phase, it is also a good idea for finance to weigh the cost versus the value of implementing the controls in the cloud to verify that there is a business case for doing so.

IDENTIFY CONTROL GAPS

Incorporating subject matter expertise from across the team, the cloud lead will document any controls that may be missing from the cloud service providers’ offerings. This gap analysis should provide a detailed accounting of every requirement and whether or not it is covered.

Security will compare the controls the cloud service provider has in place to established cloud security guidance, such as the Cloud Security Alliance Cloud Controls Matrix (CCM) and any other applicable control models. The Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ) can be a useful tool for documenting cloud service providers’ controls.

If GRC stakeholders are unable to validate that all the recommended controls are covered, they will need to communicate the risks of any gaps to the organization and further educate security on the requirements. GRC should also consider how internal rules and business controls may be affected, and whether the organization will be able to maintain the appropriate level of control over its business assets.

As any additional controls that the cloud service provider will be responsible for are identified, legal and vendor management will document them in order to be prepared to include them as part of the SLAs.
VERIFY SOLUTIONS TO FILL CONTROL GAPS

Where control gaps are identified, security and GRC will either need to work with vendor management and the cloud service providers under consideration to determine whether or not the cloud service providers will be able to fill the gaps and what will be required to achieve adequate coverage, or work with IT to determine whether they will be able to address control gaps that are the responsibility of the organization. The cloud lead will document the information about the cloud service provider’s solutions to use as part of the cloud service provider selection process.

Finance should provide a cost analysis of any controls that are added to ensure they are justified from a business perspective.
SELECT A CLOUD SERVICE PROVIDER

The cloud lead will coordinate input from all the stakeholders and oversee the organization's governance process for choosing the cloud service provider that will best meet the organization’s needs. Legal and GRC will validate that the selected Cloud service provider will enable the organization to meet all its legal and contractual obligations, compliance requirements, internal data restriction policies, insurance coverages, and other identified requirements. Security will verify that the necessary controls are in place and that the cloud service provider’s security posture is satisfactory. If the cloud service provider has limitations or is unable to customize contracts to meet these needs, these stakeholders surface those concerns to ensure that the issues will be resolved.

The various IT stakeholders will have different levels of involvement in this step depending on whether the organization is migrating to a SaaS, PaaS, or IaaS offering. These stakeholders will need to advise on the relative benefits of each option, surface the technical challenges that each presents, and help assess if cloud service provider service levels are acceptable. Exit strategies should be considered along with the measures that would be necessary in the event that the relationship with the cloud service provider comes to an end for any reason in the future.

NEGOTIATE SLAS

Vendor management will have primary responsibility for managing contract negotiations with cloud service providers. This will require an understanding of the different service and deployment models and the specific services within each offering, and it will involve considerable due diligence and working with finance to assess the costs and benefits of each option. Legal will also be involved in contract negotiations, including the establishment of penalties for failure to meet obligations and an exit strategy in the event the cloud service provider is unable to meet its commitments.

The risk stakeholder will work to ensure that the specific terms around risk mitigation and insurance coverage meet the levels that the business requires. If there are gaps, additional coverage will either need to be negotiated into the contract or the organization will need to assume responsibility for the necessary coverage. Consideration should be given to exit strategies and the potential need to build in redundancies with multiple cloud service providers if it is justified according to the risk assessment.
BUILD AS REQUIRED

Now it is time to implement any architecture that the organization is responsible for to complete the requirements of the initiative.

For SaaS applications this may be as simple as ensuring end user have access to the through the proper identity and access management channels.

For PaaS it is now time to develop and deploy the service required by the initiative. DevOps, software development, and security will advise on what the organization’s secure coding practices are.

For IaaS the architecture designed by the engineers will now be implemented in the cloud.

IMPLEMENT CONTROLS TO FILL THE GAPS

Engineering, security, and network administration will work with the cloud service provider or internal IT to ensure that the appropriate security controls are implemented to fill any identified gaps and to create mitigation plans as needed. Governance, risk, and compliance should be consulted as needed to help craft remediation plans and validate that the cloud service provider is able to implement them.

The cloud lead will oversee this process to ensure that all control gaps are addressed through design and implementation, mitigation, or acceptance.

At this time, IT (perhaps with the assistance of human resources) will also be responsible for rolling out educational materials to employees regarding appropriate, secure behaviors they will need to adhere to in a cloud environment.

LAUNCH

With all the due diligence and planning complete and any designed architecture in place, it is now time for the new cloud service to go live and become accessible to the business unit that initiated the process.
**MONITOR**

Moving to a cloud-first strategy is just the beginning of an ongoing process. Each member of the team will be responsible for contributing to the continued optimization of the cloud implementation through ongoing measurement and feedback.

As part of managing the cloud service provider relationship, vendor management should conduct regular/quarterly meetings with the cloud service provider to review the quality of service and adherence to the contract. There should also be periodic auditing to assess if the cloud service provider is still the best fit for the organization's needs.

Legal will need to periodically review the contract to assess if the cloud service provider continues to meet its contractual obligations or if any penalties or service credits should be invoked. There should also be a regular evaluation of new laws, compliance requirements, and contractual obligations and an assessment of whether or not the contract supports the new legal requirements.

As the business grows and changes, governance will need to consider if there are any impacts to the security controls that are in place. Risk and compliance will need to watch for new exposures and changing regulatory requirements, and work with security and the cloud service provider to ensure security controls and incident response plans are updated in a timely manner.

It will be important to have logging in place with the ability to detect anomalous behavior in the logs for any given service.

**ACCOUNT**

Best practice would dictate that all incidents are documented by the stakeholder that has oversight for a given aspect of the cloud responsibilities and this information will be utilized to inform future decisions made within the cloud-first deployment process model.

By providing ongoing cost analysis, finance will keep the organization informed of whether or not the cloud implementation aligns with projections.
RESPOND TO ANY INCIDENTS

Whenever anomalous behavior is detected, response plans must be initiated. For many incidents that arise a response plan may already be in place and it will be critical to initiate execution of that response plan as soon as the incident is fully understood. For any unforeseen incidents that do not have a response plan in place, it will be important to document the response to facilitate a more rapid response to that type of incident in the future.

It will be important to quickly determine whether a response is the responsibility of the organization or the cloud service provider.
Moving to a cloud-first strategy is not a single event, but rather a permanent shift in how an organization implements its business decisions. While most enterprises already have some presence in the cloud, many have made these moves without a clear process for ensuring that critical business interests are protected. Decisions that are made today will have lasting consequences for how the organization meets its legal and compliance requirements, SLAs, financial targets, and other business imperatives.

In fact, as an organization's cloud adoption increases, the outcomes of its cloud-first strategy will have an even larger impact on the business. For virtually all organizations, there will come a point when the financial burden of maintaining physical data centers and IT facilities will no longer make economic sense. Once the move has been made to cloud-only solutions, if the established cloud-first strategy does not deliver the expected cost savings, agility, and other competitive advantages, the health and survival of the organization could be at risk.

Introducing a clear and repeatable process early in an organization's cloud maturity provides the opportunity to ensure more positive outcomes as the organization progresses. By learning to engage the right stakeholders at the right time to make critical decisions, organizations will be able to create secure, efficient, and productive cloud initiatives that will support business growth and success long into the future.