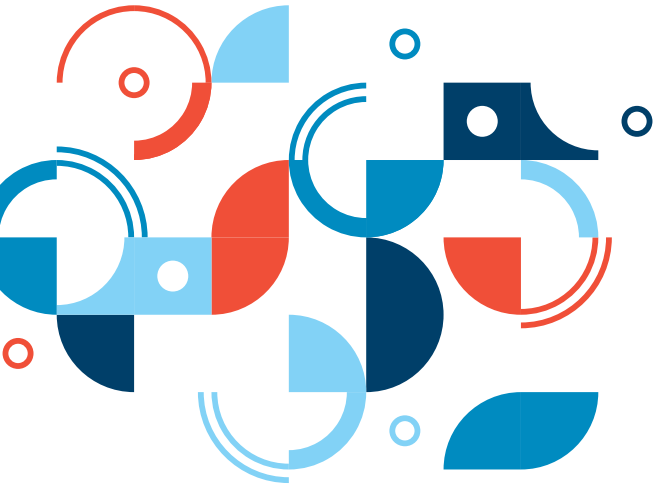
Establishing a relationship with your cloud service provider

Third in a series: Your roadmap to cloud adoption

IBM

Contents



Introduction

In the first white paper of this series, we discuss how to create a cloud computing strategy (http://ibm.co/TXqLpE). In the second white paper, we walk through the important steps of defining your cloud ecosystem (http://ibm.co/WiOqm7). Establishing a relationship with the appropriate cloud service provider (http://ibm.co/1k3alTy), covered in this paper, is the culmination of your planning and strategizing to date—the establishment of an indispensable teaming arrangement that helps you realize the business benefits defined in your cloud computing strategy.

Engaging a cloud service provider (CSP) has many similarities to engaging your typical managed service provider. CSP arrangements can also be fueled by a certain amount of anxiety around security and data protection, and migration challenges associated with the deployment of cloud delivery models. These concerns drive additional considerations and steps you'll need to incorporate into your standard procurement and managed services processes.

The surge in cloud computing implementations has led to a glut of available information about working with CSPs, and sorting through this material can be overwhelming. Although much of the information is useful, it often tends to be high level and theoretical, making it difficult to sift through the academic and tease out the practical. A concrete plan can serve as one of your best allies in the CSP journey. This paper will provide you with a list of steps and considerations that you can use as a basis for your own plan in working with a CSP.

Establishing a relationship with a cloud service provider

Issues and recommendations

Before you become a CSP client, you'll want to give some thought to key issues encountered by organizations that have already traveled down this path. Many of these considerations have been part of traditional, pre-cloud outsourcing and hosting arrangements; some are specific to cloud relationships. If your procurement organization does not have experience negotiating, establishing and managing such contracts, developing these new skills should be a priority. Below are important steps to help remediate typical stumbling blocks in a CSP relationship and achieve anticipated business value from the planned cloud environment for your organization.

Governance

- Share organizational practices with the CSP that pertain to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, test, use and monitoring of deployed or engaged services. Establish audit mechanisms and tools to support organizational practices throughout the service lifecycle.
- Confirm the CSP has all requisite certifications.
- Confirm that service-level agreements (SLAs) can be enforced and state specific remedies that apply when they are not met.

Compliance

- Understand the various types of laws and regulations that create security and privacy obligations for your organization. These could potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.
- Review and assess the CSP's offerings in the context of your requirements and examine the contract terms for adherence to those requirements.
- Evaluate the CSP's electronic discovery capabilities and processes to be certain they do not compromise the privacy or security of your data and applications.
- Confirm that the service arrangements allow visibility into the security and privacy controls and processes employed by the CSP, and the performance of these controls over time.
- Establish clear, exclusive ownership rights over data.
- Institute a flexible risk management program that will adapt to the constantly evolving risk landscape for the service lifecycle.
- Continuously monitor the security status of the information system to support ongoing risk management decisions.

Architecture

- Understand the underlying technologies that the CSP uses to provision services, including the implications the technical controls have on system security and privacy, over the full service lifecycle and across all system components.

Identity and access management

- Confirm adequate safeguards are in place to help secure authentication, authorization and other identity and access management functions, and are suitable for your organization.
- If a federated approach is planned, evaluate the tooling and interfaces necessary to provide that level of service.

Software isolation

- Understand virtualization and other logical isolation techniques that the CSP employs in its multi-tenant software architecture, and assess the risks involved for your organization.

Data protection

- Evaluate the suitability of the CSP's data management solutions for your impacted organizational data. You will also want to evaluate the CSP's ability to control access to data; to secure data while at rest, in transit, and in use; and to sanitize the data.
- Take into consideration the risk of collating your organization's data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value to cybercriminals.
- The contract should specify the CSP's obligations to your organization if any of your data becomes the subject of a subpoena or other legal or governmental request for data.
- Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the CSP.

Functionality and transparency

- An often-overlooked contract clause is a description of the service functionality you are acquiring. This clause should specify CSP requirements to provide notice prior to discontinuing a feature or functionality of its service. The notification period should allow time for your organization to implement another solution.
- Assess the risk of today's lack of standards when procuring cloud tools and solutions. For example, if you source a (public cloud-enabled) solution from vendor "A," and then subsequently have to terminate the contract and seek another provider, you should assume the transition would involve different application programming interfaces (APIs) and data formats.
- The contract should obligate the CSP to identify any functionality that it outsourced to another organization, and to whom.

Pricing

- Understand the pricing options available from the CSP. Options can include on demand or pay as you go. Another possibility is subscription pricing that can involve prepayment for reserved capacity, whether ultimately used or not. You should also consider what components are built into the pricing and what are optional. For example, network bandwidth consumption? Fixed IP addresses? Backup?

Availability

- Understand the contract provisions and procedures for availability, data backup and recovery, and check that they meet your organization's continuity and contingency planning requirements.
- Confirm that during an intermediate or prolonged disruption or a serious disaster, disaster recovery is in place, critical operations can immediately resume, and all operations can eventually reinstate in a timely and organized manner.

Incident response

- Understand the contract provisions and procedures for incident response and evaluate if they meet the requirements of the organization.
- Establish that the CSP has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
- Verify that the organization can respond to incidents in a coordinated fashion with the CSP in accordance with their respective roles and responsibilities for the computing environment.

Cloud service provider contracting activities and recommendations

A typical sourcing contract has four phases to its lifecycle: pre-contract activities, initiating activities, run-time (operational) activities, and terminating activities. Understanding the rhythm and flow to establishing a contract can help your organization

plan in advance, and navigate each phase with authority. Typically the focus is on operational activities, but equal focus needs to be placed on these three startup and shutdown phases:

Pre-contract activities

- Identify security, privacy and other organizational requirements for cloud services as criteria for selecting a CSP.
- Analyze the security and privacy controls of a CSP's environment, and assess the level of risk involved with respect to the governance objectives of the organization.
- Evaluate the CSP's ability and commitment to deliver cloud services over the target timeframe and meet the security and privacy levels stipulated.

Initiating activities

- Confirm that all contractual requirements are explicitly recorded in the service agreement.
- Involve a legal advisor in the review of the service agreement.
- Continually assess the performance of the CSP and the quality of the services provisioned to evaluate if all contract obligations are being met. Manage and mitigate risk.

Terminating activities

- Alert the CSP to any contractual requirements that must be observed upon termination.
- Understand the risks of transferring the service in-house, or to another CSP.
- Revoke all physical and electronic access rights assigned to the CSP and recover physical tokens and badges in a timely manner.
- Confirm that the organizational resources made available or held by the CSP under the terms of the service agreement are returned or recovered in a usable form, and that information has been appropriately expunged.

A hypothetical scenario and recommended approach

To move this discussion to a more concrete level, let's review a fictitious client situation that can demonstrate how our recommendations could be put into action.

Suppose an organization is looking for an analytics application and has identified a potential solution that is available via a public cloud. This would be the first public cloud-sourced service in the hypothetical organization, and as a result these typical challenges must be addressed in order to successfully evaluate the potential solution:

- Formal governance and architecture standards/processes are not in place
- Procurement has limited experience with outsourced IT solutions
- The IT organization has not worked with cloud-enabled solutions in the past

Ideally, this organization would follow these steps as it moves toward their cloud implementation. Also note that additional information about governance, workload selection, and defining a cloud ecosystem is available in the first two white papers in this series: **Creating a cloud computing strategy** (http://ibm.co/TXqLpE) and **Defining a cloud ecosystem** (http://ibm.co/WiOqm7).

Step 1. Analyze and select the workload

The process of selecting a new application (or IT service) was in play long before cloud. As illustrated in Figure 1, any new IT services should achieve technology fit, (reasonable) risk exposure and business value.

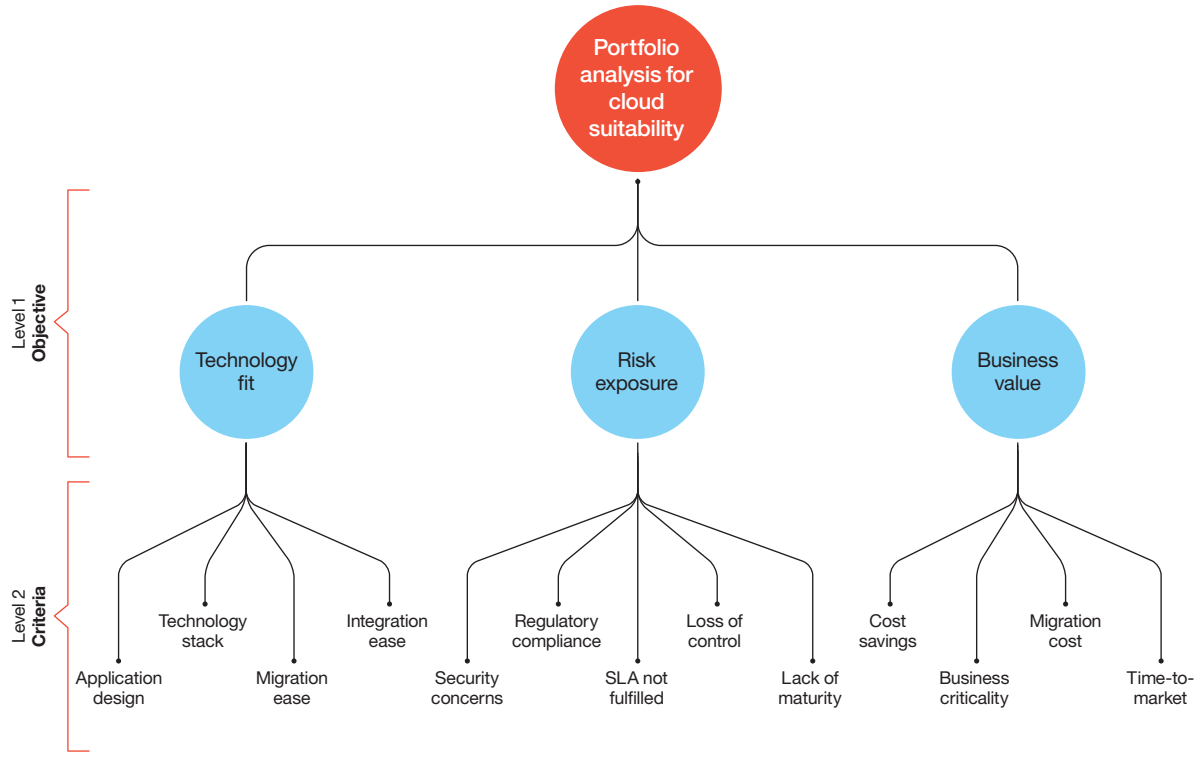


Figure 1. Objectives and criteria for analyzing a portfolio of applications for cloud suitability

In our hypothetical example, let's develop our approach for assessing the service, or workload, against these criteria:

1. Little or no need for integration with other systems
2. Unknown security and privacy controls
3. Should be available in a public cloud, pay-per-use model

Our proposed solution would appear to meet criteria around minimal integration and public cloud (although more detailed criteria will come later during contracting). However, the level of security and privacy controls represent a potential risk that should be addressed before moving ahead. Our project team needs to:

- Review the identity and role-based access controls provided.
- Review network, data and instance security features.
- Understand data location, privacy controls, data retention policy and any regulatory implications due to the planned use of data in the service.

Step 2. Establish an interim governance process

Acknowledge the risk. There is nothing wrong with pursuing the opportunity with an interim governance approach, as long as the organization recognizes the risks and senior management supports the interim governance team. It is important to identify all potential stakeholders (for example, the planning department, IT, legal and contracting) and include them in an open discussion. The organization is attempting something new. Discussion points include:

- How will we make a decision?
- Who should have a vote?
- Do we agree to share the risk?
- How will we manage the decision process?
- How will we define a successful outcome?
- How do we facilitate learning and encourage risk mitigation activities through the process?
- If applicable to only one department, should that department have the final say?

Similar considerations should be established for technical oversight if an enterprise architecture process is not in place. Some considerations will truly be requirements, such as identity and access management, security and privacy. Other considerations can be evaluated in a weighted fashion. One example could be: "The solution can only be deployed on Linux, and our standard is Windows." Both required and desired technical characteristics can be codified into a decision model, and later utilized in the evaluation process.

The bottom line: **establish an interim governance process that acknowledges the risk and is supported by senior IT and business executives.** Note that it may be appropriate to hire outside skills to augment the in-house team for skills that are not in your current inventory.

Step 3. Establish the decision framework

Designing a client-specific Software as a Service (SaaS) evaluation process would be best accomplished in a design workshop and commissioned by the (interim) governance board. The workshop participants should represent all stakeholders: IT, procurement, legal, clients, etc.

Step 4. Determine the potential business value of the proposed solution and make a go/no-go decision

Typically, the requesting department(s) would create an initial proposal for the evaluation of a new service. The template should be consistent with the client's existing planning process. Common components would include:

- A functional description of the requirements
- Requirement(s) for integration with current IT systems
- The scale or performance required, projected over the relevant time frame
- The business criticality of the service
- Is this a new or replacement service?
- Who are the intended users and what is the breadth of use? Single department? Multiple departments? External (citizen) access?
- A high-level description of the use cases envisioned
- What options are available for acquisition (i.e., traditional IT, SaaS via a public cloud provider, etc.)?
- What is the required business case/return on investment (ROI)/cost savings?
- Do key cloud attributes provide value? Self service? Flexible pricing/ability to scale up/down rapidly?
- Any known risk or technical issues?

At this point, the interim governance board would make a go/no-go decision regarding further pursuit of the opportunity.

Step 5. Determine the technology fit of the proposed solution(s)

The Enterprise Architecture Board and the agreed-upon enterprise architecture standards and guidelines for the organization provide oversight to this activity. For example, one standard could be that the service "must integrate with our identity and access system." Note that standards should represent requirements, and guidelines are desirable attributes that can be weighted and scored later in a procurement process. Typical evaluation topics can include:

- If **integrations** are required, what techniques are available? Are the interfaces open and documented? What performance and recovery mechanisms are available?
- If **migration** of existing data and services is needed, what is the level of effort and risk associated with those activities?
- Will **customization** be needed? For example, screen layouts, field names, process triggers, etc. What tools and training are available to assist?
- What is the impact to **management of the operational environment?** How will the current service management structure incorporate the new service? How are changes administered? How will billing and chargeback (if used) be accomplished?
- How **resilient** is the service? What are its availability and recovery requirements?
- Will **network latency** be a potential issue? Will additional investigation (i.e., demo, proof-of-concept) be required to evaluate?
- What **training** will be required for both end users and IT help desk staff?
- For **security** and data protection, what are the identity and access management mechanisms?
- Does the new service place **device-specific requirements** on the desktop or mobile environments?
- Do you have **information lifecycle management requirements** that must be supported by the new service?

Step 6. Determine the risk exposure (and mitigation approach) for the proposed solution(s)

This activity can be performed concurrently with Step 3, Establish the framework, as there are interrelationships between identified risk exposures and technology approaches. Risk exposure analysis typically includes the following topics:

- **Your organization's maturity level and experience with outsourcing.** Should you hire a partner or cloud service broker? Start with services at a lower risk threshold to gain experience?
- **Provider performance.** Is there an established track record for the potential CSP? Can it provide SLA terms to meet the business requirements? How easy/flexible/safe is their approach to change management? Operations? Billing/reconciliation?
- **Stability of business scenarios and use cases.** Do changes in the business processes require changes in the application, and vice versa? As a rule, if the business process definition can be extracted from the application, then SaaS is a good fit. If the opposite is true, then a business process overhaul would be a more appropriate next step.
- **Adherence to standards.** Cloud standards are nascent and evolving. Is this an issue for the service being evaluated?
- **Regulatory/legal compliance.** What legal requirements must be met, and what are the roles/responsibilities that need to be in place for both you and a potential provider? Does the SLA provide visibility into the provider's controls and processes?
- **Information management.** Will data be shared with other IT services? What is the "chain of custody?" For example, who owns the information and who can access?
- **Security.** How will data be protected, including both "in motion" and "at rest"?
- **Contractual details.** What are the contract termination provisions and exposures should you have to replace an existing provider? Is "burst" capacity anticipated, and what options would be available?

Step 7. Define the cloud ecosystem

The requirement for a cloud ecosystem will vary depending upon the cloud deployment and governance approach selected. For example, an organization might contract with a CSP to provide a Customer Relationship Management (CRM) solution that would continue to use the organization's legacy fulfillment system. This scenario of course represents a hybrid cloud model, and would require tools, processes and potential labor to successfully deploy. Please refer to the companion paper **Defining a cloud ecosystem** (http://ibm.co/WiOqm7) for additional guidance.

Step 8. Define business outcomes and use cases

The purpose of this activity is to define success in the eyes of the business owner, which could include addressing:

- What problem(s) are you trying to solve?
- What efficiencies are you trying to achieve?
- What is the financial case?
- What are the scenarios where the service will provide value (i.e., the use cases)?

This step also can bring out the requirements for training or point out effects on other processes that must be considered. Finally, this step often includes an initial business case analysis and can serve as a go/no-go decision milestone as you prepare to transition from design into implementation planning.

Step 9. Select the initial pilot

We now turn our attention to the activities that will successfully deploy the new service. Should we start with a pilot or "proof-of-concept"? Should we ask the CSP for an acceptance period before signing off on the service? How will the new service (application) be handled by our service desk?

Step 10. Develop the requirements and the procurement process

Application	• Function required • Integration needed • Privacy • Capacity • Response time • Use cases • Training
Cloud	• Identity and access management • Resiliency • Latency • Security controls • Monitoring • Logging and audit
Contract/CSP	• Price • Terms • SLA • Compliance/audit • Change process • Onboarding

Figure 2. Three key requirement areas include Application, Cloud Service and Contract/CSP

Because the proposed solution would operate as a SaaS, we need to establish our requirements in three key areas: Application, Cloud Service and Contract/CSP. (See Figure 2.)

1) The **Application category** would include specifications for the functionality required, capacity, response time, privacy and any integration with existing applications.

2) The **Cloud Service category** includes specifications that are unique to the service running in a cloud environment: identity and access management, resiliency requirements, latency and security are potential considerations. In addition, for more complex workloads, such characteristics as frequency of database backups, network bandwidth, static IP addressing, etc. can come into play.
3) The **Contract/CSP category** represents the specifications related to the outsourcing process itself such as price, terms, SLAs and more.

Step 11. Perform the procurement process

The most significant portion of the procurement process is the negotiation phase. It can be helpful to develop your list of assumptions going into the process and to include them in the procurement document itself. In addition, a key premise of cloud is the willingness to accept "standard" solutions in exchange for reduced per-transaction cost and flexibility. You may need to evaluate what level of customized features you are willing to exchange for these benefits.

Step 12. Complete the decision to pursue purchase and implementation

With the completion of the technology and risk assessments, we would subsequently make any appropriate updates to the initial business proposal. The governance board would then make the go/no-go decision to pursue an implementation. Your next steps would be unique to your budget and procurement processes. You would then continue with the process as outlined below.

Step 13. Implement the pilot project

Your contract should include either an acceptance period or a specific pilot project with exit criteria. This gives you the opportunity to gather experience, make minor adjustments and prepare for full deployment of the service.

Step 14. Roll out the transition plan

In addition to the application being deployed and associated training, your organization will need to assume a set of "integrator" responsibilities upon transition. For example:

- Help desk support
- Provisioning of new users
- Incident handling
- Limited customization capabilities (depending on the application)
- Processes associated with contract management (such as billing and reconciliation, SLA monitoring, handling of change requests, etc.) will require instantiation of appropriate process and audit controls prior to cutover

Ongoing operations

Now that you and your CSP have "gone live" in your cloud environment, you can start reaping the benefits of cloud. But unfortunately you cannot kick back and relax. You'll want to maintain vigilance over:


Transition processes


Audit and compliance activity


Periodic performance review with your CSP


Ongoing evaluation of security and data privacy measures


End of fiscal period processes


Contract renewal (and potentially termination)

Figure 3. Areas to watch as you enter ongoing operations.

Why IBM?

A solid strategy for cloud computing is critical to helping you deliver innovative IT services that can create new business value, and IBM Cloud Advisory Services can help. In fact, overall IBM was positioned as a leader in the IDC Marketscape: Worldwide Cloud Professional Services, 2013 Vendor Analysis. According to IDC's 2013 *Global Cloud Professional Services Buyer Perception Survey*,[1] clients highlighted IBM as most strong in providing functional and industry insights and competence, and using resources globally.

At IBM Cloud Advisory Services, we take a collaborative approach, weaving together business insight, advanced research and technology to give you a distinct advantage in today's rapidly changing environment. (See Figure 4.)

Our approach

With our collaborative approach, we can specifically guide you in:

- Identifying where and how cloud computing can drive business value
- Assessing the current environment to help determine strengths, gaps and readiness
- Providing a stronger value proposition for cloud computing in the enterprise
- Developing a strategy and plan to help successfully implement the selected cloud delivery model

Figure 4. IBM Cloud Advisory Services can guide you on your journey to realizing business value through a successful cloud implementation.

Our integrated perspective on cloud consulting, design and implementation can turn strategies into action. With expertise in 17 industries and global capabilities that span 170 countries, we help clients around the world benefit from new opportunities available on the cloud. To learn more, visit **ibm.com**/cloudcomputing.

IBM Cloud Advisory Services: A unique value proposition

- Positioned as a leader in the IDC Marketscape: Worldwide Cloud Professional Services, 2013 Vendor Analysis.[2] (IDC's 2013 *Global Cloud Professional Services Buyer Perception Survey)*
- Tested tools, assessments and workshops—including our unique cloud adoption framework and workload analysis tool—to help measure business impact
- Deep business and technical architecture, and data center and data center strategy expertise
- Open standards-based approach
- Intellectual capital from client cloud engagements and technology incubation projects
- Structured architecture approach
- Experience from our own transformation
- One of the broadest systems, storage, software and services portfolios in the industry to help find the right fit for your business
- The ability to deliver insights from the research conducted in our global cloud computing centers
- Extensive patent leadership

Establishing a relationship with your cloud service provider: Third in a series of white papers

You've just completed the third white paper in a series, **Your roadmap to cloud adoption**. These papers guide you through a high-level roadmap toward a future cloud design and implementation, as shown in Figure 5 below.

- **Part One: Creating a cloud computing strategy** (http://ibm.co/TXqLpE) takes you through the steps highlighted in **dark blue**.
- With **Part Two: Defining a cloud ecosystem** (http://ibm.co/WiOqm7), you will explore the topics in **light blue**.
- And **Part Three: Establishing a relationship with your cloud service provider** (http://ibm.co/1k3alTy), has covered the areas highlighted in **orange**.

The papers are designed to be used both separately and together, or with your IBM Cloud Advisory Services consultant, who can provide even more in-depth information.

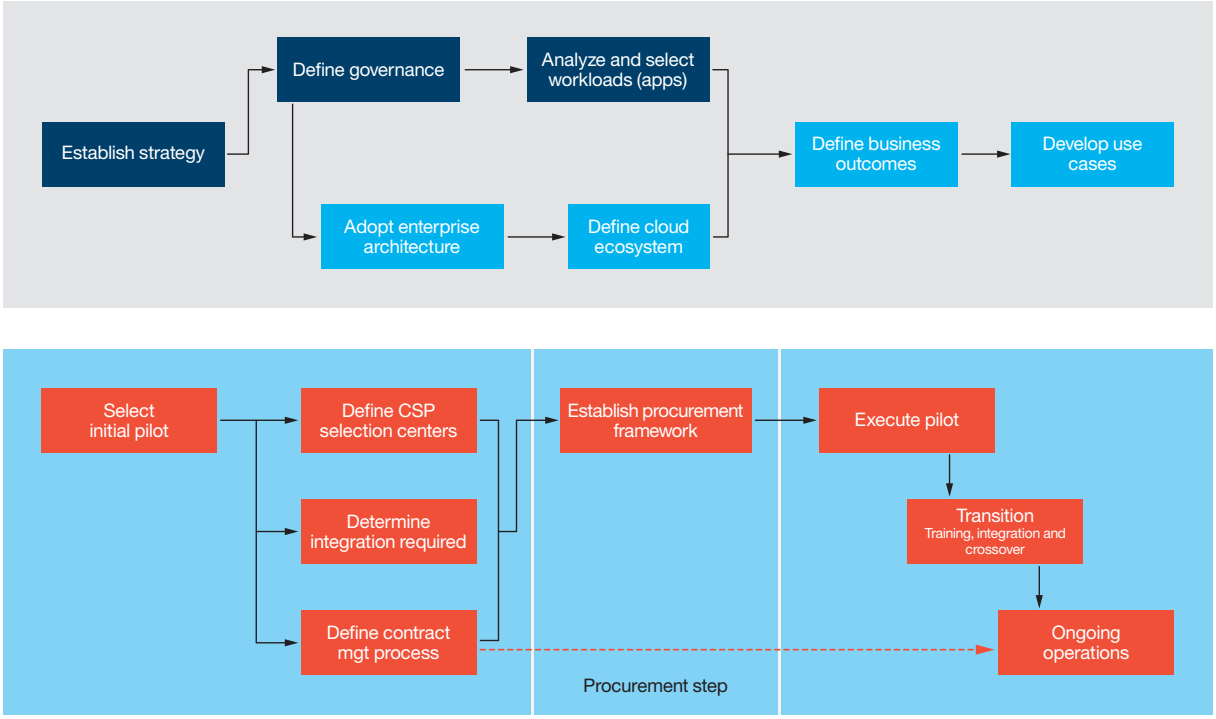


Figure 5. This is the third in a series of white papers, **Your roadmap to cloud adoption**, which guides you through the steps necessary to create a cloud adoption roadmap like the example shown here.

For more information

To learn more about IBM Cloud Advisory Services, please contact your IBM representative or visit the following website: **ibm.com**/cloudcomputing

About the author

Bob Freese is a certified consultant on the IBM® Global Technology Services® Cloud Advisory Services global team. He has over 40 years of experience in IT strategy consulting and has spent the last seven years performing cloud strategy engagements for clients and training IBM technology consultants worldwide.

IBM Corporation
Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
September 2014

[1] IDC MarketScape: Worldwide Cloud Professional Services 2013 Vendor Analysis. August 2013. IDC #242401. http://idcdocserv.com/242401e_IBM

[2] IDC MarketScape: Worldwide Cloud Professional Services 2013 Vendor Analysis. August 2013. IDC #242401. http://idcdocserv.com/242401e_IBM

Please Recycle

WUW12352-USEN-00