Abstract – The aim of this document is to provide the System Analyst a practical framework to help guide a data-informed cloud candidacy decision process. The process should result in information which university decision makers may use to clarify uncertainties and help ensure desirable outcomes in the adoption of cloud solutions.
A Cloud Strategy Framework

TABLE OF CONTENTS

1. Background and Introduction ......................................................... 3
2. Structure of this Document .......................................................... 4
3. Identifying Cloud Opportunities ..................................................... 4
4. The Assessment Process ............................................................... 6
5. The Business Case ........................................................................ 8
6. Manageability and Service Levels .................................................. 10
7. Select the Provider ........................................................................ 10
8. Preparing the Exit Strategy ............................................................ 11
9. Determining the Contractual Terms ................................................ 11
10. Prepare for Ongoing Operations .................................................... 11
11. Ongoing Review ......................................................................... 11
12. Summary .................................................................................... 12

Appendix A: Cloud Conceptual Reference Model ................................. 13
Appendix B: Assessment Survey Checklist ............................................ 14
Appendix C: Application Workload Readiness Assessment Checklist ...... 15
Appendix D: Sources ......................................................................... 16

VERSION CONTROL
Version 2015-1.0 .................................................................................. 05/21/2015
Version 2017-1.0 .................................................................................. 01/12/2017

The Cloud Strategy Framework Guide is a managed document. Changes will only be issued as complete replacement. Recipients should remove superseded versions from circulation.
1. BACKGROUND AND INTRODUCTION

Our Strategic Intent is: To drive speed, agility, collaboration, and self-sufficiency throughout the Bryant Community through the strategic adoption of cloud services.

The value of cloud service to a university is to make information immediately available, help the organization manage it, and allow the university IS organization to focus on the unique priorities within the educational environment. In the traditional IS service delivery model, there is a significant emphasis on procuring, maintaining and operating the necessary hardware/software, related infrastructure and support mechanisms. Although a cloud delivery model can enable the IS organization to focus more on innovative service creation, the operational, service management and service orchestration responsibilities still persist with all cloud delivery models; Infrastructure as a Service, Platform as a Service, Software as a service. These service manageability responsibilities either fall to the cloud provider or the cloud consumer based on the particular cloud delivery model chosen.

The essential cloud capabilities that facilitate the transition to cloud-ready IS and best position the organization to deliver innovative services are enabled by a combination of the different cloud models. In 2004, the Bryant IS service organization started on the path of adopting private cloud technologies in the datacenter for greater flexibility and higher availability. Bryant has since moved on to public cloud service offerings such as Google, and to hybrid cloud service offerings such as NaviCloud. It is fair to assume that all three cloud models will continue to play a role in delivering future IS services to the university. The illustrated Cloud Architectural Model shown in Figure 1.0 depicts how the different models need to integrate and interact in order to deliver on the promise of an on-premise cloud enabled IS infrastructure. It’s essential that the various design and development groups within the IS organization align future plans with the cloud model blueprint.

Figure 1.0 Cloud Model Blueprint
A Cloud Strategy Framework

The intent of this document is to put forth a framework to be used in evaluating a delivery model for application workloads and services so they may be sourced from the most reliable, timely, economical, and secured environment available to the university. The framework can be used to assess such IT services in identifying their readiness for the cloud. The advantage of adopting a framework in assessing cloud candidacy, is to provide detailed traceability and due diligence that clearly and confidently justifies the outcomes.

Not every use case need undergo the entire framework process. There will be instances where, due to inherent characteristics of the use case, and/or ample supporting evidence available to support the use case, undergoing the full process would likely only aid to corroborate the known.

2. Structure Of This Document

The document contains reference to the different cloud models and their principles of operation. Understanding these models helps all cloud participants better understand the technical and non-technical aspects associated with assessing cloud service candidacy. The remainder of this document steps the assessor through the various stages of the assessment framework. The document also includes supporting materials in the appendices for the assessor’s review. Appendix A lists a Conceptual Cloud Reference Model. Appendix B lists an Assessment Survey Checklist. Appendix C lists an Application Workload Readiness Assessment Checklist. Appendix D is a list of the referenced documents.

3. Identifying Cloud Opportunities

While it’s essential that Information Services leads the development and management of the university’s cloud strategy, there needs to be a coordinated approach between Information Services, university units, and all represented stakeholder groups, in identifying the opportunities that would benefit from cloud-based services. An overriding principle in deploying a cloud strategy is that one size doesn’t fit all. Information Services in conjunction with the appropriate university units must invest the time and effort to identify cloud opportunities and choose the cloud services model that best-fit the application workload and ultimately the business process. It is difficult if not impossible to generalize a best-fit cloud model for application workloads without assessing the individual use case. The first step is to evaluate application rationalization - why are some applications and services a better fit than others? Application workload requirements need to be assessed not only in terms of functionality but in terms of availability and scaling. It’s essential that the assessor understand the full impact of moving an application workload to the cloud, or sourcing a service directly from the cloud.

Generally speaking, the different cloud service model segments provide different types of value to the consumer. The different models differentiate themselves by providing direct and indirect value to the consumer within the different layers, as shown in Figure 2.0. The illustration also marks the distinction between cloud provider responsibilities and cloud consumer responsibilities for each of the cloud services models.
3.1 A Structured Approach

The approach outlined in this document is in line with a cloud-first strategy as opposed to a plan-backward build-forward strategy. The approach assumes that it makes the most sense for the university to consider cloud services case-by-case, as new requirements present themselves or at the next iteration of an existing application or service; rather than considering the entire portfolio of existing applications and services at a single point in time. There are several advantages to this approach. Cloud providers, cloud carriers and cloud brokers will continue to evolve and mature with new and innovative services, making it difficult to roadmap an entire portfolio of services to what would be considered a point-in-time “target state”.

A case-by-case approach allows us to take into consideration circumstances that make the individual analysis unique along a progressing cloud maturity timeline. With each case, the value derived from cloud benefits will likely be different, such as savings, continuity of operations, the value of new capabilities the cloud model has to offer, and the readiness and capabilities of the organization to make the transition.

Some examples of likely candidates for the assessment process include:
- Business and IT systems scheduled for replacement;
- Planned system implementations/upgrades;
- Requirements for system development/testing where cloud infrastructure could be used;
- Pilots, time-bound or short lifespan projects; and capabilities used only periodically;
- Significant hardware refresh;
- Software renewals;
- New applications;
- Application augmentation (new functionality);
- Case of significant process change.
4. THE ASSESSMENT PROCESS

4.1 Assessment Survey
The case for identifying cloud computing opportunities can be made by following a structured decision assessment process. By following a structured process you should arrive at a much more informed decision point. This approach includes checklists that help guide the overall assessment process.

The first step in the process is to perform an initial assessment survey of the application workload under consideration for cloud candidacy by using the Assessment Survey Checklist. Information gathered by the survey is meant to provide a very general indication of the application’s potential for cloud.

4.2 Application Workload Readiness Assessment
A favorable or sometimes even a seemingly unfavorable assessment survey will lead to the next step, an application workload readiness assessment. Assessing application workloads for cloud readiness allows us to determine what applications and data can – and cannot – be readily moved to a cloud environment and what delivery models (public, private, or hybrid) can be supported. Rationalizing which applications go to the cloud and which to leave on premise is determined according to your unique requirements and decision criteria. Your decision criteria may in fact be refined as the assessment progresses.
A Cloud Strategy Framework

The readiness assessment takes into account considerations outlined in sections below. Taking these aspects into consideration the assessor is asked to conclude a cloud readiness favorability rating, using the Application Workload Readiness Assessment Checklist.

4.2.1 Business Considerations
Business considerations include the overall organizational readiness for using cloud computing. Is the application owner willing and comfortable with a cloud platform? How important is the application to the business or the mission? What is the risk tolerance level of the business unit, and is the culture favorable or resistant to change? Will there be disruption to existing business processes?

4.2.2 Application Lifecycle Considerations
Is the application still being defined? Is it up for a refresh? Is the application approaching retirement? Can the application be redesigned or undergo a technology refresh, be modernized for cloud computing, optimize business process? Will there be gains (efficiency, innovation, agility, competitive differentiation, etc.) in using a cloud model? Instead of migrating the existing application to cloud computing using an IaaS or PaaS approach, would it be better to replace it with a new SaaS solution or new architecture?

4.2.3 Application Architecture Considerations
Is the application web-based, or built with a service-oriented architecture (SOA)? If not, is the application such that it can be split into modular services? Is it monolithic, two-tier, three-tier, or n-tier? What is the level of effort required to modularize it or separate the tiers? Does the application scale out? Does it scale up? What are the demand fluctuations in the application? What impact if any will moving to cloud have on demand?

4.2.4 Data Considerations
Data governance, confidentiality, integrity, availability and quality need to be preserved by the migration. Is the data bound by compliance regulations? Are there data sensitivity and privacy or confidentiality concerns? What data integrity concerns are there? How does the application manage data requests from a safety and security perspective? How much data exchange will occur between the components of the application and between the application and the user? Will frequent data transfers impose a higher cost or a performance lag?

4.2.5 Technology Considerations
These include the performance and resiliency of the underpinning infrastructure to support the application (networks, storage, compute, security, facilities, etc.). Does the migration design account for multiple components communicating across network boundaries (logical, physical)? Is the application designed (or can it be modified) for resiliency - immunity to the interruption of transactions in midstream? Is the application designed for high availability and/or fault tolerance? Finally, standard and open protocols are more readily supported across cloud and public infrastructures than proprietary ones – does the application support standard and open protocols?

4.2.6 Security Considerations
All cloud participants – application owner, cloud service provider and university IT – must understand that security is a joint responsibility. Authentication and authorization should remain the responsibility of the university at the application level. The cloud service provider is responsible for security controls, identification and correction of system vulnerabilities, and
defense against specific cloud-oriented threats. Continuous monitoring, end-to-end service monitoring is now common among cloud service providers and should be expected.

### 4.2.7 Integration Considerations
What are the dependencies between the application and/or service being migrated and other systems? Applications may depend on each other through control integration (they invoke each other), data integration (they read or write to the same databases or files), or presentation integration (they are mashed up on the same window or Web page). The migrated application workload may even be the “system of record” for some key data in a data management scheme. The migrated application may rely on common facilities such as a user directory for single sign-on and access control. The assessment must discover how extensive these integrations are, what protocols they use, what additional utilities or runtime libraries they may rely on, and what their performance requirements are, including the frequency of connections and the amount of data involved. Will there be a need for connections between the migrated application and applications and data that remain in-house, potentially requiring new integration software?

### 4.2.8 Data Backup and Archiving Considerations
If cloud storage is the primary storage for the application consider that most online storage and/or managed service providers do not provide a separate secure archived copy to protect files from accidents, such as an employee deleting a wrong folder, or attacks, such as all contents of your online drive being maliciously destroyed or held for ransom by a bad-actor. In order to assure the availability and integrity of the data, a secondary copy of the data should be preserved by following a methodology similar to on premise backup and archival standards.

## 5. THE BUSINESS CASE

Once an application workload is assessed as favorable for cloud computing, a thorough business case needs to be developed. The work that goes into building a business case and the business case content ultimately becomes your business communications package, your “bridge” document, to win support for the case.

Developing a business case requires specific information that describes the current state of the application workload and demonstrates the advantages of the cloud delivery model for the specific use case. The high level value propositions for cloud computing include faster speed of deployment, scalability, and value delivery beyond the capabilities of the IT organization. With certain use case cloud applications there could be a potential cost savings when considering the complete financial impact, total cost of ownership, the application and its required ecosystem exerts on the organization. Individual business problems and/or opportunities with existing applications that cloud computing can potentially address, need to be identified and quantified, and specific business justification must validate that the cloud model is the right alternative.

The business case should provide an objective view of the business rationale, benefits, costs, risks and options involved with determining a cloud solution alternative. The business case should weigh cloud against other alternatives, such as non-cloud solutions. The case justifies the appropriateness of the cloud solution for the specific use case and will provide a reference point for re-evaluation at a future point in time.
5.1 Building a Business Case
The business case takes into account considerations outlined in the following sections:

5.1.1 Business Rational Summary
Executive level summary of the business rational for creating or moving the application workload to cloud services.

5.1.2 Proposed Solution
Present sufficient detail to allow decision-makers to evaluate the business solution. For example: range of solutions considered; reasons solution is recommended; direct and indirect benefits; evidence that the cloud solution meets the stakeholder’s needs; evidence of prior success elsewhere.

5.1.3 Cost Analysis
Describe the investment required to implement the proposed solution. Consider such items as:
- Start-up and ongoing cloud service costs;
- Any additional costs to handle peak loads or scaling beyond the norm;
- Show the return on investment (ROI) and/or added value, describe any opportunities where ROI benefits strategically position the university for future gains;
- Estimate the cost over a defined period of delaying of not proceeding with this initiative;
- Any costs associated with application re-design changes to accommodate this solution;
- Any fees associated with service management from the cloud provider such as backup, archiving, bandwidth, transaction volume, etc.;
- Any fees associated with licensing or license management;
- Costs associated with application workload integration, testing and deployment;
- Description of the project framework – key roles and responsibilities, skill requirements, duration of main activities;
- Any additional pertinent business factors.

In order for a meaningful comparison to be made, you should include the baseline costs of any current environment.

5.1.4 Assess the Risks
Identify and assess the expected risks to which this cloud solution will be exposed. Describe the risks that could affect the solution. Using the Information Services Risk Register indicate the sources of risk. The Risk Register includes the following:

- **Strategic risk** - is risk that affects an organization's ability to achieve its goals;
- **Financial risk** - is risk that may result in a loss of assets;
- **Operational risk** - is risk that affects an ongoing management process;
- **Compliance risk** - is risk that affects compliance with externally imposed laws and regulations as well as with internally imposed policies and procedures concerning safety, conflict of interest, and the like;
- **Reputational risk** - is risk that affects an organization's reputation, brand, or both.

Finally, outline a plan to manage the risks identified for each use case.
5.1.5 Critical Success Factors
List the factors needed to ensure success of the proposed cloud solution. Be specific, include items such as: management commitment; business unit engagement; project team staffing and resources; training; etc.

5.1.6 Criteria for Measuring Success
Describe how the success of the cloud solution will be tracked, measured and reported. The metrics should be based on the following criteria:

- Meaningful – The metric must be understood by the recipients;
- Accurate – A high degree of accuracy is essential;
- Cost effective – The measurements should not be costly to acquire or maintain;
- Repeatable – The measure must be reliable over time;
- Predictive – The measurement must be indicative of outcomes;
- Genuine – Not random or subject to manipulation.

To promote consistency with this process, a standardized business case template should be used in developing the business case document. Also, consider a high-level presentation document to be included as a business case deliverable for presentation purposes.

6. MANAGEABILITY AND SERVICE LEVELS

In addition to the business case, it’s equally important to ensure that the level of service provided by the cloud-based solution will be comparable to current service levels in the case of an existing application workload or service, and will meet required service levels in the case of a new application workload or service. The required service levels should be agreed with the cloud service provider and explicitly documented in the cloud service agreement. Consider such items as described below:

6.1 Application Availability
The criticality of the application to business operations will determine the availability requirements that must be clearly specified in a cloud engagement document.

6.2 Application Performance
Depending on the performance requirements of the application, specific performance targets may need to be achievable with the cloud service.

6.3 Application Security
Moving an application to the cloud will require due diligence on the part of the cloud provider to ensure proper security controls are in place and operating effectively.

6.4 Privacy and Regulatory Compliance
Personally Identifiable Information (PII) handled by a cloud-based application must be properly stored and maintained. Access to PII and sensitive data stored in a cloud service must be restricted as required by regulatory bodies, Bryant’s institutional data protection standards, and any other situational related compliance constraints.
7. Select The Provider

Selecting the cloud service provider involves verifying the following: that the business needs are fully satisfied; assuring the pricing model is transparent; the cost model is confirmed and suitable, the provider allows for scaling and changes to service; security requirements are fully addressed; setup, training and integration activities are confirmed, customer references are checked; all commitment requirements are contained in the contractual agreements.

8. Preparing The Exit Strategy

It’s important to develop an exit strategy that considers business scenarios that have a likelihood of occurrence. For example: inability of the service provider to meet the agreed upon levels of performance; business viability issues with the provider that could cause interruptions in service delivery; a security breach; an opportunity to move to a more attractive provider; etc.

9. Determine The Contractual Terms

As is the case with most cloud service providers, expect to be presented with a standardized “click wrap” agreement. It’s important that a standard protocol is followed and contracts adhere to the university’s vendor management guidelines and vetting process. The processes mentioned will ensure that individuals that better understand specific university contractual requirements are given the opportunity to amend the agreements with the terms and conditions necessary for the particular use case.

10. Prepare For Ongoing Operations

Ensure the internal capabilities required to manage and support the cloud service are available, documented and ready to be and put in place for daily ongoing activities. Such activities might include: all parties acknowledging the IS service owner; monitoring performance and service levels; documenting incident response and incident escalation protocols (Run Book activities); coordinating and implementing changes; establishing protocol to reconcile deficiencies in service, be it cost or performance related. Ensure all commitments for operational hand-off are in place.

11. Ongoing Review

It’s highly recommended that the analyst undertaking this assessment record and document all steps of the process, including those steps where a checklist is not provided. The documentation will serve as a reference point for future (ongoing) reviews of the use case. The documentation will also be used as feedback to help improve the process over time.

As part of the ongoing process, the IS owner should continue to manage the vendor relationship. All interactions with the vendor should be recorded throughout the lifecycle of the service. It’s important to capture and record the service provider’s ability to respond to changing conditions and requirements, their
attentiveness and response to Bryant concerns and their supply side performance. Such information tracked over time will become invaluable in the ongoing evaluation of the service provider.

Lastly, the IS owner should ensure that periodic risk assessments are undertaken for information held in the cloud, and periodically compare the value and benefits of the service to the costs, in light of changing conditions.

12. **SUMMARY**

Readers of this document should note that despite the guidelines provided in this document, the ultimate selection of cloud solutions and their success depend upon the judgment of IS and the business decision makers. Furthermore, organizational realities present during the decision timeframe will have significant influence in the decision making process.

Please keep in mind, the overall process outlined in this document does not exclude systems and applications from the full Systems Development Lifecycle (SDLC) process. The cloud computing approach and traditional SDLC are similar. It’s the duration and the importance of the various stages of SDLC that will differ between approaches.
**APPENDIX A: CLOUD CONCEPTUAL REFERENCE MODEL**

**TERMS**

Cloud Consumer - Person or organization that maintains a business relationship with, and uses service from, Cloud Service Providers.

Cloud Provider – Person, organization or entity responsible for making a service available to service consumers.

Cloud Carrier – The intermediary that provides connectivity and transport of cloud services between Cloud Providers and Cloud Consumers.

Cloud Broker – An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

Cloud Auditor – A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
## APPENDIX B: ASSESSMENT SURVEY (CHECKLIST)

### Assessment Survey

<table>
<thead>
<tr>
<th>General Indicators</th>
<th>Cloud Option vs Traditional Application, System, Service</th>
<th>Likely To</th>
<th>Comments/Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Increase</td>
<td>Neutral</td>
<td>Decrease</td>
</tr>
<tr>
<td>Overall Cost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Savings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational Overhead</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software licenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University Software License</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Requirements (supply side)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Benefits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud agility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flexibility of Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Composite Implementation (Integration, Scaling, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opportunity to adopt existing cloud based services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Degree of Confidence</td>
<td>High</td>
<td>Reasonable</td>
<td>Low</td>
</tr>
<tr>
<td>Cost %</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely To</td>
<td>Increase</td>
<td>Neutral</td>
<td>Decrease</td>
</tr>
<tr>
<td>Success Indicators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business needs &amp; objectives</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investment Objective</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Requirements</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic Fit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adherence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Degree of fit (supply side)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Indicators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business practices are understood and adapted to cloud based service delivery</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commercial agreements are understood</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity to meet University standards (supply side)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical applications are present in the educational vertical</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service and support organizations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity to meet Security and Compliance Obligations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Degree of Confidence</td>
<td>High</td>
<td>Reasonable</td>
<td>Low</td>
</tr>
<tr>
<td>Overall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost %</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Application Workload /Service:**

**Analyst:**

**Date:**

Cloud Strategy Framework
## APPLICATION WORKLOAD READINESS ASSESSMENT (CHECKLIST)

### Application Workload Readiness Assessment

<table>
<thead>
<tr>
<th>Category</th>
<th>Reliability Index</th>
<th>Performance Score</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Lifecycle Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Architectural Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration Considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Favourability Rating</th>
<th>0%</th>
</tr>
</thead>
</table>

### Availability Rating

- Below 65%: Unfavourable for Cloud
- Between 65% and 75%: Neutral Improvement
- Above 75%: Favourable for Cloud

### Reliability Index (Importance)

- 1 - Critical
- 2 - Important
- 3 - Modestly Important
- 4 - Least Important
- 5 - Not Important

### Notes:

Application Workload / Service:

Analysis:

Date:

Cloud Strategy Framework
APPENDIX D: SOURCES

NIST Cloud Computing Reference Architecture
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

NIST Cloud Computing Standards Roadmap

NIST Cloud Computing Security Reference Architecture
http://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf

Cloud Strategy for Higher Education: Building a Common Solution
http://www.educause.edu/library/resources/cloud-strategy-higher-education-building-common-solution

Migrating Applications to Public Cloud Services: Roadmap for Success

http://www.cloud-council.org/PG2CC_v2.pdf

Cost and Business Case Considerations

A Guide to Implementing Cloud Services

Strategies for Evaluating Cloud Computing Agreements, Bloomberg Law Reports

Cloud 101: Developing a Cloud-Computing Strategy for Higher Education