IBM Center for
The Business of Government

Using Technology Series

Cloudy with a Chance of Success

Contracting for the Cloud in Government

Shannon Howle Tufts
Meredith Leigh Weiss
University of North Carolina
at Chapel Hill

Using Technology Series 2013

Cloudy with a Chance of Success: Contracting for the Cloud in Government

Shannon Howle Tufts
Meredith Leigh Weiss
University of North Carolina at Chapel Hill

IBM Center for
The Business of Government

Table of Contents

Foreword

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, *Cloudy with a Chance of Success: Contracting for the Cloud in Government,* by Shannon Howie Tufts and Meredith Leigh Weiss, University of North Carolina at Chapel Hill.

Daniel J. Chenok

With the movement of government activities to leverage cloud computing, government agencies are now increasingly writing and negotiating contracts with cloud service providers. While agencies have been writing and negotiating contracts for many years, contracts for cloud services present a special set of challenges. In this important report, Shannon Tufts and Meredith Weiss present a detailed analysis of 12 major issues that need to be addressed in all cloud contracts. In addition to traditional issues such as pricing, cloud computing contracts require that a variety of data assurance issues be addressed, including data ownership, access to data, disposition of data, data breaches, and data storage location.

Thomas Richey

This report is based on a detailed analysis of five public sector contracts in North Carolina for cloud services. The five case studies included a local government, a state agency, a higher education institution, a local public health organization, and a K-12 public school system. Based on these case studies, the authors developed a series of recommendations for government organizations to guide them in the writing and negotiating of contracts for cloud services.

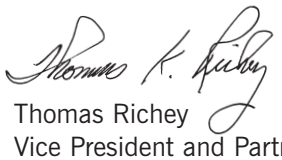
Dr. Jane L. Snowdon

With the publication of this report, the IBM Center for The Business of Government continues its ongoing interest in cloud computing. In 2012, the IBM Center published *Mitigating Risks in the Application of Cloud Computing in Law Enforcement* by Paul Wormeli. That report addressed the concerns about cloud computing in the law enforcement community. Many of the concerns discussed in the Wormeli report are also addressed in this new report. In 2009, the IBM Center published *Moving to the Cloud: An Introduction to Cloud Computing in Government* by David C. Wyld. That report addressed 10 major challenges facing government in implementing cloud computing. These three

reports serve as major resources for government managers as they increasingly move more activities to the cloud.

We hope that both government managers and contract officers will use this timely and informative report as they develop contracts for cloud services in the years ahead.

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com



Thomas Richey
Vice President and Partner
Public Sector Cloud and Infrastructure Services
IBM Global Business Services
trichey@us.ibm.com

Dr. Jane L. Snowdon
Director and Chief Innovation Officer
IBM Federal
snowdonj@us.ibm.com

Introduction

Tight budgets have forced federal, state, and local governments to seek cost-effective methods for delivering technology solutions. Many of these governments are exploring or implementing cloud-based technologies, which provide on-demand services via the Internet (Wyld, 2009). As governments move toward cloud-based solutions in hopes of cheaper, faster, and better technology applications and services, a series of issues related to contracting for the cloud are emerging (Barnes, 2010; Gates, 2009; Joint and Baker, 2011).

This study assesses five public sector cloud contracts in the state of North Carolina. The case studies are assessed against commonly identified best practices for cloud computing and legal/regulatory requirements to determine how the contracts were negotiated and whether all necessary conditions were met in the contract vehicle.

The report begins with a brief overview of cloud computing, including its benefits, challenges, and the need for high-quality computing contracts. Second, a framework for assessing public-sector cloud computing contracts is discussed, including legal/regulatory requirements as well as standard best practices. Third, five government case studies are presented and analyzed. Finally, lessons learned are presented.

The analysis of contract issues, decision-making processes, and lessons learned culminate in the development of a framework for negotiating cloud contracts in the public sector that can be used by governments and cloud providers alike.

An Overview of Cloud Computing

In simplest terms, cloud computing refers to the delivery of computing services over the Internet from a remote location (Wyld, 2009). Computing clouds, which provide these services, are collections of easy-to-use, accessible virtualized resources that can be simply reconfigured to match demand, allowing for optimal use of resources (Gatewood, 2009). Cloud services are commodity services that operate on a one-to-many model, whereas outsourcing is typically a highly customized service, tailored to a customer's requirements (Andrew and Baker, 2011).

Cloud Computing Benefits

There are numerous benefits to cloud computing, which include:

- **Increased capabilities,** such as rapid deployment, easy implementation, access to higher-level information technology (IT) resources, disaster recovery, and remote and mobile access
- **Enhanced efficiencies**, such as scalability, flexibility, agility, just-in-time delivery, resource utilization, automatic updates, fewer duplicative systems, and increased reliability
- **Reduced cost**, such as fewer infrastructure investments (hardware, software, maintenance, upgrade, refresh, day-to-day operation), physical space savings, improved economies of scale, and usage-based pricing

In addition, cloud computing is good for the environment (Andrew and Baker, 2011; Barnes, 2010; Kundra, 2011; Scruggs et al., 2011; Wyld 2009).

Cloud Computing Challenges

The increased capabilities, enhanced efficiencies, and reduced costs offered by cloud computing must be weighed against its numerous risks (Wyld, 2009).

- First, cloud services are exploding and decisions need to be made as to when cloud service shall be used. It is projected that there will soon be thousands of cloud vendors. To remain competitive as these resources grow, it is critical that government be adept at strategically determining when to cloud source.
- Second, security, including network security, data protection, privacy, physical security, and application security from cloud providers raise security concerns for information technology executives.
- Third are data issues including ownership, confidentiality, access, format, and portability; as well as vendor lock-in (dependency on the vendor), and vendor viability.
- Fourth, dynamic and changing cloud services must be monitored to ensure proper performance and benefit realization. Service level agreements, therefore, must be drafted and managed properly.

- Fifth, vendor contract negotiation is complicated and critical. There are few customer cloud agreement templates; therefore legal issues, combined with compliance and regulation requirements, compound the challenges of cloud computing (Scruggs et al., 2011).

In 2012, the U.S. Government Accountability Office issued a report on the progress of cloud migration efforts in the federal government (GAO, 2012). In the report, seven common challenges are identified, including meeting federal security requirements, obtaining guidance, acquiring knowledge and expertise, certifying and accrediting vendors, ensuring data portability and interoperability, overcoming cultural barriers, and procuring services on a consumption (on-demand) basis.

Contract Considerations for Cloud Computing in the Public Sector

To realize the potential opportunities afforded by cloud computing and address many of its challenges, it is particularly important to concentrate on the establishment, negotiation, and management of high-quality cloud computing contracts. Far too often, organizations in both public and private sectors sign Master Service Agreements or standard contract documents without properly reviewing, negotiating, and modifying the terms and conditions of the contract to meet the subscribing organization's needs and legal requirements.

This report will highlight many of those common oversights by documenting a public sector cloud computing contract reference framework, drawn largely from the work of Scruggs, Trappler, and Philpott (2011), and supplemented through additional academic and legal research. The resultant framework is used to assess the cloud computing contracts of five public sector organizations in the state of North Carolina to ascertain common areas of concern and opportunities for improvement. Interviews with staff members in each organization added rich contextual detail to the understanding of the trade-offs and considerations used as contracts for cloud services were established and negotiated.

A Framework for Assessing Public Sector Cloud Computing Contracts

As governments move toward cloud-based solutions seeking cheaper, faster, and better technology applications and services, a series of issues related to contracting for the cloud have emerged (Barnes, 2010; Gates, 2009; Joint and Baker, 2011). While cloud computing is becoming more common among government and other public sector entities, it carries a multitude of legal and regulatory considerations that impact the effectiveness of public sector contracts. Cloud computing offers additional layers of complexity due to issues including data assurances, offsite storage of data, and public records requirements.

Some of the major legal and regulatory challenges facing government in negotiating cloud computing contracts include:

- Physical data location and its effect on determination of jurisdiction and applicable law
- Privacy and confidentiality requirements
- Electronic discovery requirements
- Security requirements
- Breach disclosure requirements
- Data ownership and access requirements

Each of these challenges is included in the framework presented in Table 1 for assessing cloud computing contracts.

The framework was developed to assess the five public sector cloud contracts examined in this report. Much of this framework was derived from the seminal work of Scruggs, Trappler, and Philpott (2011), and through careful analysis of other academic and legal publications and recommendations (Barnes, 2010; Bradshaw, Millard, and Walden, 2011; Joint and Baker, 2011). The framework highlights 12 major assessment areas.

Table 1: Cloud Computing Contract Assessment Framework

Major Issues for Cloud Contracts	Description of Specific Elements
1. Pricing	• Pricing Caps (limit on pricing increase over time) • Pricing Changes Notice (requirement to give notice prior to pricing changes) • Pricing Changes Time Frame Limitation (limitation on how many pricing changes can occur within set time frame) • Demand Pricing (requirement to match lower pricing offered to other similar entities when quantities, services, etc., are comparable) • Costs for Special Services/Additional Quantities/Etc. (costs related to items not specifically included in the original contract scope)
2. Infrastructure Security/ Right to Audit and Inspect	• Financial Audit/Review • Performance Audit • Infrastructure/Data/Security Assurances (broadly stated) • Security Monitoring Practices (Logical and Physical) • Data Segregation Practices • Operations Management Requirements • Employee Approval Processes for Sensitive Data • Third-Party Audit and Inspection of Physical and Logical Security • Review of Company Audit Logs, Event Logs, Testing Results Related to Physical and Logical Security (including specifications and topology diagrams) • Forensic Access
3. Data Assurances	• Data Ownership: data custody, intellectual property, exclusion of data mining or selling, data processing ownership • Access to Data: consent to access, government access and retrieval at sole discretion, process for access/retrieval • Disposition of Data Upon Request: destruction authority, audit process • Disposition of Data Upon Termination: data provision process, obligation to transfer, common data format, destruction authority, audit process • Data Breaches: notification process, vendor obligations, government obligations, indemnification, remediation/penalties • Data Storage Location: Physical data storage requirements, data segregation requirements • Litigation Holds: metadata/imaging, legal cooperation clause, data preservation/media preservation, cost allocation, redaction process, data provision process • Public Records Requests (FOIA Requests): data provision process, redaction process
4. Governing Law, Jurisdiction, and Forum Selection	• Specified as North Carolina Pursuant to NC G.S. 22B-3

Table 1: Cloud Computing Contract Assessment Framework (continued)

Major Issues for Cloud Contracts	Description of Specific Elements
5. Service Level Agreements (SLAs)	• Definitions • Parameters/Performance Requirements • Monitoring and Auditing for SLA Compliance • Technical Support • Acceptable Use • SLA Violation or Non-Performance Penalties Notice • Specification of Remediation and Penalties for Non-Compliance
6. Outsourced Services	• Requirement to Inform Customer of Outsourced Functions • No Assignment of Contract without Express Written Permission • Approval of Subcontractors
7. Functionality	• Description of Functionality • Notice of Substantive Changes • Customer Right to Replace Product or Terminate Due to Substantive Changes
8. Disaster Recovery/ Business Continuity	• Minimum Requirements • Notification Process • Inspection and Audit (covered under Technical Audit/Inspection) • Penalties (covered under SLAs)
9. Mergers and Acquisitions	• Notice of Pending M&A • Assignment Rights • Contract Binding Upon M&A • Continuity of Service
10. Compliance with Laws, Regulations, and Other Standards	• Specifications of Applicable Governing Laws • Specifications of Applicable Regulatory Requirements • Direct Liability • Indirect Liability • Limitations of Liability • Warranties • Indemnification
11. Terms and Conditions Modification	• Notice of Modification
12. Contract Renewal and Termination	• Renewal Options • Obligation to Transfer • Contract Release Without Show Cause • Suspension of Services • Non-Appropriation Clause • Advance Notice of Contract/Service Termination by Vendor • Escrow Language

Major Contract Issues Confronting Cloud Computing

Case Study Descriptions

Five North Carolina public sector cloud computing contracts were selected for assessment and inclusion in this report. Each was selected because of the unique nature of its contracts, the varying levels of involvement in contract negotiation and oversight by key public sector staff members, and the variety of cloud-based applications sought. Four of the five contracts are currently in place in the various jurisdictions. One jurisdiction terminated negotiations with the proposed vendor due to legal and technical challenges that could not be resolved.

Case One: A Large Local Government in North Carolina. The jurisdiction sought to leverage a cloud environment for its e-mail and e-mail archiving environment. Approximately 4000 user accounts and 800 GB of storage were required as part of the cloud solution, along with security, reliability, and other standard terms and conditions for hosted e-mail environments. The local government's estimated contract amount was $450,000 over the duration of the contract. The local government did not sign the contract and terminated negotiations after critical legal and technical assurances could not be met. However, this jurisdiction had substantial involvement from legal and IT professionals during the negotiation process and their near-final contract is quite comprehensive.

Case Two: A State Agency in North Carolina. The agency entered into a contract for a cloud-based enterprise forms and digital signature service. The estimated cost of the contract was $780,000 over the duration of the contract and allowed for approximately 100,000 seat subscriptions for the cloud-based solution.

Case Three: A Public Higher Education Institution. The organization leveraged a cloud-based case management system. The software as a service solution provided a web-based time, document, and collaboration management platform. The service was provided at no cost to the institution and without a user limit or term.

Case Four: A Local Public Health Department. The department leveraged a cloud-based e-mail solution for its organization. The organization is composed of approximately 200 e-mail user accounts, but the contract did not include archiving or backup for the e-mail solution. The total cost of the contract was $25,000 annually.

Case Five: A K-12 Public School System. The school system entered into a cloud contract for a suite of applications including e-mail for approximately 650 end users. The majority of the application services were offered at no cost, with only the e-mail archiving and discovery functionality charged for. The total cost of the contract was $7,150 annually.

The five selected case studies offer insight into issues affecting all major segments of the public sector, including local government, state government, post-secondary education, public health, and K-12 education. Each selected case is using or attempted to use cloud computing offerings

as part of its IT operational framework. In one case, the local government example, the city did not finalize its contract for cloud services due to a variety of legal and technical barriers. The four remaining cases are still actively engaged in the use of the cloud offerings for which they had contracted. Each of the 12 issues from the framework presented in Table 1 is described in the following sections, as well as recommendations based on case study findings.

Issue One: Pricing

Overview

Negotiating pricing carefully at the onset is critically important. Pricing for cloud services typically includes initial or upfront costs, maintenance and continuation costs, renewal costs, and volume commitments. Expansion or reduction of usage pricing may also be included in this category, as well as minimums, penalties, and special services.

Findings from Case Studies

Table 2 summarizes the pricing contract terms assessed for each of the five case studies.

Table 2: Pricing Elements in Five North Carolina Public Sector Cloud Contracts

Pricing Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Pricing Caps (limit on pricing increase over time)					
Pricing Changes Notice (requirement to give notice prior to pricing changes)	●		●	●	
Pricing Changes Time Frame Limitation (limitation on how many pricing changes can occur within set time frame)				●	
Demand Pricing (requirement to match lower pricing offered to other similar entities when quantities, services, etc., are comparable)					
Costs for Special Services/ Additional Quantities/Etc. (costs related to items not specifically included in the original contract scope)	●	●		●	

● = Organization included this feature in their cloud contract.

As seen in Table 2, none of the five contracts include language to reflect pricing caps. One contract has language that limited price changes to occurring once per year, with language similar to the following excerpt:

> "Customer will pay Company X the fee(s) set forth on Exhibit A to this Agreement in accordance with Section 3.2. Company X will have the right to change the fee once per year, effective with the next renewal date. Company X will notify Customer of any fee increase at least 45 days prior to the expiration of the then-current term."

In this example's language, the pricing increase is not limited, but notice is required within a reasonable time frame to allow the government entity to find alternative solutions for the cloud offering if the pricing increase is too substantial. Two contracts have language that allows pricing changes to occur at any time during the duration of the contract with notice. In one contract, the pricing change notice is specified as 30 calendar days, while the other contract simply states, "All prices are subject to change upon notice."

Three of the five contracts include specific provisions related to special services or additional quantities pricing. For example, one contract states, "Customer agrees to pay Company's then-current rates and expenses, including the cost of any vendors, for any requests related to information retrieval, subpoenas, consulting and advisory services or similar work."

Recommendations

A variety of pricing assurances should be included in cloud contracts. Clearly, cost per unit or contract costs should be articulated in the contract, and all contracts evaluated had inclusions related to total or unit pricing. However, the contract should include specific price caps to eliminate ballooning costs after the initial investment. For example, a fee increase cap of 3% over a one-year period, or restricting price increases to once a year with a set limit on total price increase, is a wise practice. Additionally, contracts should include provisions to adjust pricing downward if the identical services (including functionality, quantities, and total contract cost) are provided to other government clients at a lower cost. In the framework for cloud contract assessment, this is termed demand pricing, but may also be referred to as price matching.

In addition to pricing caps and demand pricing, cloud contracts should also include specifications on pricing for special services, additional quantities, and the like. Finally, greater detail and specification related to additional quantities or special services should be used in all cloud contracts, especially related to items such as information retrieval related to public records or Freedom of Information Act requests. Specifically, we recommend:

- **Recommendation 1a:** Contractually codify, in advance, costs to continue using as well as those to expand the volume of use.
- **Recommendation 1b:** Pre-negotiate costs to expand and be cautious when it comes to volume commitments. Avoid purchasing more than needed or paying for services earlier than required.
- **Recommendation 1c:** Carefully set minimums as not to become locked in to a particular vendor or incur penalties.
- **Recommendation 1d:** Investigate tiered usage discounts when beneficial.
- **Recommendation 1e:** Make sure costs for special services such as eDiscovery, additional storage, and transition services are included.

Issue Two: Infrastructure Security Requirements/Right to Audit and Inspect

Overview

Privacy and confidentiality of data is another substantial area of concern from a legal and regulatory standpoint, and is closely related to infrastructure security assurances. In a 2011 survey conducted by Ernst & Young Global Management, 77% of respondents stated that cloud computing made it more difficult to ensure privacy (p. 26). There is often a level of ignorance on the part of cloud users about the security requirements imposed on them, but it is the responsibility of the user, *not the provider,* to "impose all legal or regulatory requirements that apply to [the] enterprise … Taking the HIPAA regulations as an example, any subcontractors that you employ (for example, a cloud services provider) must have a clause in the contract stipulating that the provider will use reasonable security controls and also comply with any data privacy provisions" (Winkler, 2012).

Infrastructure security includes the supplier's responsibilities in the areas of information security, physical security, operations management, and audits and certifications.

- First, information security sets out responsibilities and obligations related to securing customer information. These responsibilities may include providing secure gateways, conducting audit and penetration tests, installing security monitoring systems, ensuing data segregation between customers, using encryption, and providing identity and access management.
- Second, physical security obligations might include security policies, response plans, access controls, surveillance, intrusion detection, multi-factor authentication, staff background checks, staff training, segregation of staff duties, and monitoring of third-party adherence to security policies.
- Third, effective data center operations management includes asset management processes to ensure proper vulnerability patching; change management processes that minimize disruption, data loss, and damage; system access limitations; proper capacity and resource planning; effective data replication, storage, distribution, and recovery; and effective virtual server provisioning and management (Scruggs, Trappler, and Philpott, 2011).

Audits and certifications confirm that infrastructure security practices meet contractual requirements and best practices. Certification examples include:

- Statement on Standards for Attestation Engagements
- Service Organization Controls
- International Standards Organization

This section of the contract codifies the customer's rights to inspect or contract a third party to inspect the supplier's services, systems, and data centers, as well as the customer's rights to conduct a vulnerability scan or other test of supplier systems and facilities. Furthermore, it outlines the supplier's obligations to conduct third-party data integrity audits. This area of the contract often includes vendor recertification requirements, the supplier's obligations to modify infrastructure to meet obligations, and the time frame under which customers will be provided audit and certification reports (Scruggs, Trappler, and Philpott, 2011).

Case Study Findings

Infrastructure security requirement and auditing components recommended for cloud contracts include specifications about security monitoring practices (logical and physical), data segregation

requirements, employee approvals for access to sensitive customer data, operations management, third-party audit allowances, customer review of such audits, onsite inspection and/or penetration testing, and access or review to specifications and topologies to ensure adequate security measures are in place, and forensic access if necessary.

Table 3 offers a summary of the various elements assessed with respect to infrastructure security and the right to audit and inspect.

In terms of financial auditing, two of the contracts specify proof of financial stability and viability from the cloud provider. Example language includes, "The Vendor shall provide evidence of financial stability, defined as financial statements for the past three (3) fiscal years, including income statements, balance sheets, and statement of charges in financial position or cash flows." Similar language is found in most public sector contracts. However, when entities use a vendor-supplied master service agreement and/or service level agreement, or accept "click through" contract terms, the financial audit/inspection component is rarely included in the contract language. In reviewing the case studies regarding the right to audit the performance records of the cloud provider, as well as access to daily and weekly service quality statistics, we found that only one of the five contracts clearly articulated this requirement within the contract document.

All five contracts include a brief statement about logical and physical security, typically assuring the customer that the cloud provider uses the highest levels of security to protect customer data. Only two of the contracts include specific statements or requirements related to security monitoring practices. For example, one contract states, "employ information security best

Table 3: Infrastructure Security/ Right to Audit and Inspect Elements in Five North Carolina Public Sector Cloud Contracts

Security & Technical Audit/ Inspection Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Financial Audit/Review	●	●			
Performance Audit	●				
Infrastructure/Data/Security Assurances (broadly stated)	●	●	●	●	●
Security Monitoring Practices (Logical and Physical)	●	●			
Data Segregation Practices	●				
Operations Management Requirements		●			
Employee Approval Processes for Sensitive Data		●			
Third Party Audit and Inspection of Physical and Logical Security		●			
Review of Company Audit Logs, Event Logs, Testing Results Related to Physical and Logical Security (including specifications and topology diagrams)	●	●			
Forensic Access					

practices with respect to network security techniques, including but not limited to, firewalls, intrusion detection, and authentication protocols, vulnerability and patch management." If the contracting organization is dealing with sensitive data in its cloud environment, special attention to security monitoring, audit logs, and other regulatory or legal compliance requirement should be included.

Only one contract specifies data segregation requirements, namely that the government entity's data reside "on servers that contain only government data." This requirement is of critical importance for government entities that perform public safety functions. This contract is the sole example specifying operational management requirements, such as requiring all data to "be held in FISMA certified, fully encrypted data centers located within the United States." Finally, only one contract specifically articulates employee approval requirements, namely reserving the right to "conduct a security background check or otherwise approve any employee or agent provided by the Vendor."

Recommendations

Government entities engaging in cloud services should specify their right to request third-party audits and/or certifications related to infrastructure and security, including penetration testing and vulnerability assessments, in the contract. Only one contract studied for this report includes such language, stating, "Upon thirty (30) business days' notice to Vendor, an independent third party auditor mutually acceptable to both Parties will have the right to conduct an on-site audit of the System on behalf of Customer and at Customer's sole expense." Additional contract language follows, specifying how such audits will occur and the requirements for confidentiality and compliance requirements for any such audit.

Two of the five contracts articulate that any reports produced from security audits and certifications will be provided to the public sector entity for review. None of the contracts specifically outline the right of forensic access to the vendor facility, equipment, etc., in the event of a criminal investigation related to a breach of customer-owned data within the cloud environment. Specifically, we recommend:

- **Recommendation 2a:** Require proof of financial stability and viability from cloud provider.
- **Recommendation 2b:** Specify any particular security requirements related to security monitoring practices, especially if required by other federal, state, or local regulations or policies.
- **Recommendation 2c:** Specify data segregation requirements, if needed.
- **Recommendation 2d:** Contractually codify the right to request third-party audits and/or certifications.

Issue Three: Data Assurances

Overview

Data assurances are a critical component of contracting for the cloud. There are a multitude of issues related to data assurances, including ownership, access, disposition, storage location, and litigation holds. These issues include:

- **Ownership:** Data ownership refers to the legal custody, control, and/or possession of data. In the context of cloud contracting, this section of the contract will establish the public sector's ownership of its data stored in the cloud.
- **Access to Data:** Data access typically defines those persons in an organization who have the authority to view or retrieve organizational data housed in the cloud. A complicated

issue of data access related to the 1986 Stored Communications Act (SCA) is currently being debated across various courts in the United States. The SCA was originally enacted to provide Fourth Amendment-like privacy protections for certain electronic communications and computing services. The Act generally prohibits government agencies from compelling disclosure of certain electronic information from third-party service providers without obtaining a warrant, court order, or administrative subpoena. Although court rulings have varied over the past few years in terms of applicability of this Act to the cloud environment, many cloud providers have chosen to require that governmental customers maintain end-user consent in order to access information housed within their cloud services, e.g., a cloud e-mail offering.

- **Disposition of Data Upon Request and Upon Contract Termination:** Data disposition refers to the procedures and processes used to destroy data when the contracting entity requests such destruction or a contract is terminated by either party.
- **Data Breaches:** A related set of legal issues that must be addressed before making the move to the cloud is what happens in the event of a security breach (Hogan Lovells, p. 15). Most states have data breach laws stating that the data host—in this case, the cloud service provider—must notify the data owner of the breach, but not the individuals affected by the breach (Stevens, 2012, p. 3). However, the state may require governments and businesses notify consumers in the event of a security breach of a consumer's personal information—unless the personal information has been encrypted or redacted in a manner that renders the information unusable or unreadable to third parties, as found in North Carolina under the 2005 Identity Theft Protection Act. If the breach occurred within a cloud environment, it would likely be incumbent upon the government entity as the original collector of the consumer data to perform such notifications, unless otherwise specified in the contract. While no one wants to think about data breaches, they are an unfortunate reality of electronic data, as outlined in a 2012 Congressional Research Service report (Stevens, 2012).
- **Data Storage Location:** Another legal issue to be considered before a move to the cloud is the physical location of the data. The actual location of the servers being used to store the data can have substantial legal ramifications for several reasons. Jurisdiction governing the data and determining applicable law is one major concern. Cloud service providers (CSPs) may have "different rules related to compliance and disclosure from region to region, or … a homogenous global cloud" (Ernst & Young, 2011, p. 5). For example, many countries have variations in laws governing privacy and confidentiality of data, particularly personally identifiable information (e.g., health and banking records), as well as intellectual property rights. If the agency or entity that created the data is in one place and the data is stored elsewhere, does the law of the agency's locale or the server's locale apply? (Mills, 2009, p. 7)
- **Legal Data Holds/Public Record Requests:** Compliance with public records laws and legal data holds is also a core part of cloud contracts. Specifically, this section of the contract references who has the authority to release public records, processes and procedures for requesting and producing such records, and obligations related to legal hold requirements. Electronic discovery is another major legal consideration prior to entering cloud contracts. Under the 2006 Federal Rules of Civil Procedure amendments, particularly FRCP 34, the discovery of electronically stored information (ESI) is explicitly authorized. According to the committee note to FRCP 34, the definition of ESI is "intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."

  The above definition allows discovery obligations to adjust to new technologies and, at least in theory, prevents litigants from evading discovery obligations by claiming that the

definition of document does not keep pace with the technological changes. However, this electronic discovery requirement complicates issues of cloud computing in that governmental (or other organizations') legal counsel have an obligation to become familiar with their client's ESI in order to comply with discovery duties of identifying, preserving, and producing relevant information. This familiarity requirement in the cloud environment presents substantial challenges in terms of understanding how information is transmitted and stored, accessing such information, and data retention requirements and practices, as well as backup policies and procedures of said cloud vendor. Contractual obligations related to electronic discovery typically include creating ESI data indices, documentation of data storage policies and practices, and clear requirements related to the cloud vendor's requirements for preservation and provision of information (Joint and Baker, 2011).

Case Study Findings

Table 4 highlights the elements of each category, as well as the findings from the cloud contract content analysis. All five of the contracts include vague language related to data access and retrieval requests and thus more specification is needed in the contract. Only one of the five evaluated contracts includes disposition language, and in that example, the contract clause is vague.

Three of the five contracts include some detail related to data retrieval or return upon termination, but none specifies common formats for data retrieval. Additionally, most of the contract language relate to disposition of data was included by the cloud provider to limit the amount of time the customer had to retrieve the data once the contract ended. One contract states, "All of your data may be irrevocably deleted within fourteen (14) calendar days of termination." None of the contracts include contract language to require the vendor to destroy all government data after contract termination, or asserting the government's right to conduct an audit to ensure the data have been destroyed.

The majority of the cloud contracts studied include provisions related to data breaches. However, none offers specific reporting/notification requirements related to the breach within a specified timeline, as well as details about the breach such as its nature, the data compromised, the involved parties, mitigation efforts, and corrective actions to be taken by the vendor. Additionally, all of the contracts include clauses to protect the vendor from any liability arising from breaches.

Two of the five contracts examined include clauses about data residing within the United States. One of the five contracts specifies a communication process for informing the government of any legal requests (including public records requests), as well as mechanisms to ensure that the data is preserved in its entirety during the duration of the litigation.

Recommendations

Data Ownership

Cloud contracts should clearly state that the government owns all of its data residing in the cloud. Typically, the contract language will include rights to government data ownership related to issues such as intellectual property, and will disallow access of the data for corporate gain by the cloud provider or organizations other than the government. An example of contract language related to data ownership is: "This Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property." One area routinely neglected in all of the examined contracts is the ownership of data processing information created when the public sector entity's data was in transmission, storage, etc. This area should also be included in cloud contracts with specific ownership of that data clearly in the domain of the customer entity. Specifically, we recommend:

Table 4: Data Assurances Elements in Five North Carolina Public Sector Cloud Contracts

Data Assurances Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Data Ownership: data custody, intellectual property, exclusion of data mining or selling, data processing ownership	●	●	●	●	●
Access to Data: consent to access, governmental access and retrieval at sole discretion, process for access/retrieval	●	●	●	●	●
Disposition of Data Upon Request: destruction authority, audit process			●		
Disposition of Data Upon Termination: data provision process, obligation to transfer, common data format, destruction authority, audit process		●	●		●
Data Breaches: notification process, vendor obligations, government obligations, indemnification, remediation/ penalties		●	●	●	●
Data Storage Location: Physical data storage requirements, data segregation requirements		●			●
Litigation Holds: metadata/ imaging, legal cooperation clause, data preservation/media preservation, cost allocation, redaction process, data provision process	●	●	●	●	●
Public Records Requests (FOIA Requests): data provision process, redaction process	●	●	●	●	●

- **Recommendation 3a:** Contractually codify that the public sector entity owns all of its data residing in the cloud, including data processing information.

Access to Data

The public sector entity should be able to access and retrieve its data stored in the cloud at its sole discretion, including the right to access all data regardless of content creator. Sample contract language found in many of the assessed documents states, "the Jurisdiction may, at any time, access and retrieve all data stored in the Cloud." One specific clause that should be considered relates to the Stored Communications Act of 1986 and governmental access to content created by its employees. Common example language found in two of the contracts is "Customer's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: Customer's access, monitoring, use and disclosure of this data and Vendor providing Customer with the ability to do so."

The contract should specify how the data will be retrieved from the cloud in the event of an emergency or time-sensitive situation, with specific procedures and timelines noted. In all cases involving data access and retrieval requests, the contract should specify the process by which the government will validate the request, including positions within the government authorized to make such a request and to whom within the cloud provider. Specifically, we recommend:

- **Recommendation 3b:** Specify the right of identified positions within the organization to access and retrieval of data stored in the cloud, regardless of content creator.

Disposition of Data

There are two situations in which the issue of disposition of data arises, either:

- Upon request from the government
- Upon contract termination

Cloud contracts should provide a mechanism for the government to require the cloud provider to destroy specified records as requested. The purpose of this mechanism is to allow the government to destroy records when allowed by law (e.g., according to the retention schedule) and not have additional copies of the records residing in other locations, such as the cloud, which would then make the records subject to disclosure upon public records requests or in the event of litigation.

In the event of contract termination, by either party, specific instructions **should** be included in the contract to determine how data will be returned or retrieved. Specifically, we recommend:

- **Recommendation 3c**: Describe processes and procedures for data disposition upon contract termination or organizational request, including audit authority to ensure data destruction has occurred.

Data Breaches

These clauses typically state: "Vendor will not be liable for any harm that may be caused by the execution or transmission of malicious code or similar occurrences, including without limitation, disabling devices, drop dead viruses, time bombs, trap doors, Trojan horses, worms, viruses and similar mechanisms." The contracts also include language to hold the public sector entity liable for any breaches that arise due to customer accounts being compromised or similar malware being introduced by the customer. Specifically, we recommend:

- **Recommendation 3d:** Clearly articulate the processes and procedures to be followed in the event of a data breach, including notification requirements, timelines, detailed information about such breaches, and remediation activities.

Data Storage Location

The legal system cannot keep pace with technology and, currently, some courts are holding that the legal jurisdiction over a contract dispute involving data takes place in the state where the data physically resides. North Carolina has a law (G.S. 22B-3) that voids contract provisions that require disputes under the contract to be litigated outside of the state, but it is important to consider the inclusion of statements about the physical storage location of government data (particularly requiring the data to remain within the United States). Contracts should specify governing law to help ameliorate these potential challenges related to jurisdiction. Specifically, we recommend:

- **Recommendation 3d**: Specify data storage location requirements, if predicated by law, regulations, or governing policies.

Litigation Holds/Public Record Requests

Litigation holds and public records responsibilities are also critical and should be included in contracts for cloud services. The contract clause must also include clear requirements related to offsite or backup media used, which can be included in the scope of an electronic discovery process. Furthermore, cloud contracts should specify that the cloud provider will not provide data to individuals, groups, or organizations making records requests unless directed to do so by an authorized government official. Sample language found in one contract states, "Customer is responsible for responding to Third-Party requests. Vendor will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request in a manner permitted by law; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request." Specifically, we recommend:

- **Recommendation 3e:** Include language and procedures related to public records (or Freedom of Information Act) requests and legal data holds.

Issue Four: Governing Law, Jurisdiction, and Forum Selection

Overview

The contract outlines the governing law by which any legal disputes will be settled and the jurisdiction (place) where the dispute will be decided (Scruggs, Trappler, and Philpott, 2011).

Findings from Case Studies

Two of the five contracts specifically reference North Carolina law and require venue for any legal actions to occur within the specific county of the signing public sector entity. One contract remains silent on both governing law and venue for arbitration and/or litigation. The remaining two contracts specify the home state of the cloud provider as the location for any legal actions, as noted in this contract language, "Any claim or suit arising out of or relating to this Agreement will be brought in any court of competent jurisdiction located in the County and State of New York." Table 5 summarizes the findings.

Table 5: Governing Law/Jurisdiction/Forum Selection in Five North Carolina Public Sector Cloud Contracts

Governing Law/Jurisdiction/Forum Selection Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Specified as North Carolina pursuant to NC G.S. 22B-3	●	●			

Recommendations

Government contracts should specify the governing law by which any legal disputes will be settled and the jurisdiction (place) where the dispute will be decided. North Carolina General Statutes (NC G.S. Section 22B-3) voids contract provisions that require disputes under contracts to be litigated outside of the state and sets North Carolina as the location for dispute resolution. However, most vendor-supplied contracts will name the home state of the vendor as the venue for legal arbitration and/or litigation or the contract will remain silent on venue. Specifically, we recommend:

- **Recommendation 4:** Contractually codify both governing law and venue for arbitration and/or litigation.

Issue Five: Service Level Agreements (SLAs)

Overview

Service level agreements describe the measurable service parameters provided by the cloud supplier, which include:

- **The level at which they are to be provided.** These parameters typically include such items as availability, performance/response time, error correction time, and quality of service.
- **Definitions and service inclusions/exclusions.** Inclusions and exclusions may address such topics as uptime, downtime, scheduled maintenance, calculations, and recover time and point objectives.
- **Monitoring and reporting expectations.** Monitoring and reporting includes performance reporting and auditing. It designates how service levels are measured (who measures, how it is measured, how often it is measured) and how that information is provided to the customer. It also dictates the customer's rights to review service level measurement records.
- **Remedies when service obligations are not met.** The remedies section of the contract addresses what the cloud provider must do in the event the SLAs are not met. These include items such as root causes analysis, corrections, penalties, assessing/applying financial penalties, bonus/malus, or other remedies (Scruggs, Trappler, and Philpott, 2011).

Case Study Findings

Service Level Agreement components are prevalent and detailed across all five contracts. However, many of the contracts use vendor-provided SLAs as part of the contract document with little to no negotiation, thereby potentially reducing the effectiveness of the SLAs for the customers.

The five North Carolina contracts were analyzed for both SLA violation or non-performance penalties, as well as for specification of damages and credits. Three of the five contracts include language for both elements of remediation and penalties as noted below in Table 6.

Table 6: Service Level Agreement Remediation and Penalties Elements in Five North Carolina Public Sector Cloud Contracts

Remediation and Penalties Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
SLA Violation or Non-Performance Penalties Notice	●	●		●	
Specification of Remediation and Penalties for Non-Compliance	●	●		●	

Similar language regarding SLAs is contained in the three contracts, but the following example is offered as a sample: "Subject to valid submission of a Service Availability Credit request and the other conditions herein, if Service Availability under Your Account for any calendar month is below 99.999%, credit will be issued in accordance with the following schedule: 99.00%-99.9999% equals 3% of the month fee credited…" A common concern with remediation and penalties is whether the customer organization negotiated the terms of the SLA and the terms of the remediation and penalties or if they simply accepted the vendor's prescribed terms.

Recommendations

Cloud contracts should specify service level parameters, minimum levels, and specific remedies and penalties for non-compliance with SLAs. Typical items for inclusion in SLAs are uptime, performance and response time, error correction time, and infrastructure and security requirements. Public sector entities need to ensure that the SLA clearly defines the pertinent terms, such as downtime, scheduled downtime, etc. These definitions eliminate ambiguity in contract enforcement and provide specific mechanisms for calculating compliance with the SLA.

Remediation and penalties are also functions of *or* result from well-defined SLAs. Cloud contracts should include corrections and/or penalties for non-compliance or non-performance related to the established SLAs. Both corrections and penalties should be specific, such as: "Service credit will be rendered when SLA is not met by the vendor. The service credit will be applied as liquidated damages against the following quarter of service costs." It is important to document how the credit will be provided and when it will be provided. Ideally, the financial penalty should be 10–20 percent of the contract in order to motivate the vendor to avoid violations. These penalties should be related to SLA performance, while fines and costs associated with data breaches should be covered under the Data Assurances section of the contract. Specifically, we recommend:

- **Recommendation 5:** Specify service level parameters and remedies/penalties for non-compliance with SLA terms.

Issue Six: Outsourced Services

Overview

It is not uncommon for a cloud provider to outsource certain aspects of their business. This section of a cloud contract typically focuses on the obligations of disclosure and approval for outsourced services or functionalities. Additionally, non-assignment clauses, which ensure the cloud vendor remains directly responsible for all aspects of contract compliance despite outsourced components, are found in this contract section (Scruggs, Trappler, and Philpott, 2011).

Case Study Findings

Many government contracts require approval for the use of subcontractors, particularly if those subcontractors work outside the United States. One of the case study contracts includes such a clause, specifying "the Vendor may subcontract the performance of required services with other Vendors or third parties provided that Vendor notifies the Customer in writing in advance … and will do so only with the prior written consent of the contracting authority." Table 7 outlines the elements assessed with respect to outsourced functions or services.

Table 7: Outsourced Services Elements in Five North Carolina Public Sector Cloud Contracts

Outsourced Services Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Requirement to inform customer of outsourced functions	●	●			
No assignment of contract without express written permission	●	●			
Approval of subcontractors		●			

Recommendations

The cloud contract should require the vendor to inform the government of any outsourced functionality and its provider. The contract should also require the cloud vendor with whom the contract is signed to remain directly responsible for all terms of the contract, regardless of outsourced functions, unless otherwise approved in writing by the governmental entity. In other words, the contract should specify that assignment is either disallowed or only allowed with express written permission. For example, the following language pertaining to assignment is used in one of the North Carolina contracts: "Neither party may assign or transfer any part of this Agreement without the written consent of the other party." Specifically, we recommend:

- **Recommendation 6:** Require the cloud provider to notify the public sector entity of any and all outsourced functionality, including specification related to assignment or non-assignment of responsibilities articulated in the contract to outsourced or contracted organizations.

Issue Seven: Functionality

Overview

Functionality of the product or service refers to the actual services being received or performed, rather than simply the name of the product.

Case Study Findings

All of the contracts evaluated include functionality descriptions in the contract or the original Requests for Proposal, which became part of the contracts as modified Statements of Work. In terms of notification of functionality changes and the right to replace or terminate, all contracts include language related to functionality changes, but the majority do not require notification of changes. For example, one contract specifically states that the vendor "can modify or discontinue, temporarily or permanently, any feature associated with the Service, with or without notice."

The four contracts with similar language also include language stating that "continued use of the Service after modification constitutes acceptance of the changes and continuation of the contract." Conversely, two of the contracts specifically protect the governmental entity from substantive functionality changes by requiring advance written notification of thirty (30) calendar days, with an option to replace the service or terminate the contract prior to the implementation of the functionality changes or modifications. Table 8 details the findings of the functionality contract language assessment.

Table 8: Functionality Elements in Five North Carolina Public Sector Cloud Contracts

Functionality Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Description of Functionality	●	●	●	●	●
Notice of Substantive Changes				●	
Customer Right to Replace Product or Terminate Due to Substantive Changes				●	

Recommendations

It is important that cloud contracts state the functionality of the product/service being purchased in order to maintain continuity across technological and branding changes. As technology changes and products are rebranded, it is important not to lose functionality or be forced to switch to a new product at a higher cost. Included in the contract should be the description of the functionality, a requirement for advance notice if it is to be changed or deleted, and a notification period so that there is time to switch (Scruggs, Trappler, and Philpott, 2011). Specifically, we recommend:

- **Recommendation 7a:** Contractually codify the functionality of the services procured from the cloud provider.
- **Recommendation 7b:** Specify required notices for substantive functionality changes, including contract termination procedures if functionality alterations do not meet the needs of the public sector entity.

Issue Eight: Disaster Recovery/Business Continuity

Overview

Disaster recovery and business continuity clauses specify the required processes, procedures, and safeguards to protect the contracting public entity's data and services in the event of system failures.

Case Study Findings

None of the contracts evaluated offer specific contract language related to Disaster Recovery and Business Continuity requirements. Breach notification requirements are found, but those are covered under Data Assurances. Additionally, right to inspect and audit is covered under Technical Audit and Inspection, while penalties are covered under SLAs.

Table 9: Disaster Recovery/ Business Continuity Elements in Five North Carolina Public Sector Cloud Contracts

Disaster Recovery/ Business Continuity Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Minimum Requirements					
Notification Process					
Inspection and Audit (covered under Technical Audit/ Inspection)					
Penalties (covered under SLAs)					

Recommendations

It is critically important that the service provider has adequate disaster recovery (DR) and business continuity (BC) processes in place to recover from a natural or manmade disaster. First, the contract should cover what the minimum DR/BC mechanisms in place are, as well as a commitment as to how long it will take to recover from a disruption. Second, in the event of a service interruption, it is important to know how long it will take to switch to a backup site, the level of service and functionality provided by the backup site, and within what time frame the provider will recover the primary data and services. Third, the contract should specify how and how often the data are backed up. Backup reports should be generated to

monitor vendor's performance. Fourth, the cloud provider should test their DR/BC processes at least annually and provide results to the customer. Fifth, DR/BC procedures should be in place, communicated, and tested for any third-party providers being used. Finally, the contract should specify the provider's obligations in terms of notification, failover processing, problem correction, and reimbursement if a service is interrupted/ceased, and/or a data loss/breach occurs (Scruggs, Trappler, and Philpott, 2011). Specifically, we recommend:

- **Recommendation 8a:** Cloud contracts should specify minimum disaster recovery and business continuity requirements and ensure that the cloud provider meets the minimums through inspection of documentation, onsite audits, etc.
- **Recommendation 8b:** The contract should specify penalties for failures in complying with the minimum requirements, as discovered through onsite inspections, audits, or actual disasters.

Issue Nine: Mergers and Acquisitions

Overview

Mergers and acquisitions clauses articulate the responsibilities and transferability of contracts or contract terms and conditions in the event of a corporate merger or buy-out.

Case Study Findings

As seen in Table 10, only one of the five contracts contains provisions about mergers and acquisitions, including notice requirements, non-assignment without express written permission of the contracting authority, binding terms for the new company, and continuity of service requirements in the event of a merger or acquisition.

Table 10: Mergers and Acquisitions (M&A) Elements in Five North Carolina Public Sector Cloud Contracts

M&A Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Notice of Pending M&A					●
Assignment Rights					●
Contract Binding Upon M&A					●
Continuity of Service					●

Recommendation

One commonly overlooked area for contract provision relates to mergers and acquisitions. Cloud providers in particular are prone to such market activity and any cloud contract should define notice requirements, assignment rights, and whether contract terms are binding on successors. Specifically, we recommend:

- **Recommendation 9:** Contractually state that the terms are binding on successors and neither party may assign, delegate, or otherwise transfer its obligations or rights without prior written consent of the other party (Scruggs, Trappler, and Philpott, 2011).

Issue Ten: Compliance with Laws, Regulations, and Other Standards

Overview

Compliance with laws, regulations, and other standards clauses is included in contracts to ensure the government entity obligates the cloud services supplier to federal, state, and local requirements. Examples of these requirements include United States laws such as Gramm-Leach-Bliley, Sarbanes-Oxley, HIPPA, and FERPA; state laws; laws of countries where the customer conducts business; and standards such as the payment card industry (PCI) data security standard (Scruggs, Trappler, and Philpott, 2011). Additionally, standard cloud contracts tend to disclaim warranties, and are often overlooked in contract negotiations.

Case Study Findings

All five contracts have boilerplate language related to such compliance, warranties, and liabilities provisions. These provisions are not the same as those noted in the aforementioned Governing Law/Jurisdiction/Forum Selection section. The only area of concern is Specifications of Applicable Regulatory Requirements, where only three of the five contracts include such language (the local government contract, the state agency contract, and the public health contract).

Table 11: Compliance with Laws, Regulations, and Other Standards Elements in Five North Carolina Public Sector Cloud Contracts

Compliance with Laws, Regulations, and Other Standards Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Specifications of Applicable Governing Laws	●	●	●	●	●
Specifications of Applicable Regulatory Requirements	●	●		●	
Direct Liability	●	●	●	●	●
Indirect Liability	●	●	●	●	●
Limitations of Liability	●	●	●	●	●
Warranties	●	●	●	●	●
Indemnification	●	●	●	●	●

Recommendations

All government contracts for services or products should include provisions ensuring the vendor complies with all governing laws, regulations, and other specified standards of import to the contracting entity, as well as contract language related to warranties and liabilities, as required by federal, state, or local governing law. Examples of warranties to consider negotiating include: services warranty, compliance with laws warranty, disabling code warranty, warranty of authority, third-party warranties and indemnities, date/time change warranty, most-favored customer warranty, and performance and/or compliance with specifications or requirements warranty (Scruggs, Trappler, and Philpott, 2011). Specifically, we recommend:

- **Recommendation 10a:** Contractually codify that the cloud provider must comply with all governing laws, regulations, or other specified standards of importance.
- **Recommendation 10b:** Clearly specify required warranties and liabilities, pursuant to appropriate governing law.

Issue Eleven: Terms and Conditions Modification

Overview

Terms and conditions refer to the rules that are followed as part of procuring a cloud service. Quite often, cloud contracts incorporate terms and conditions found at a specific URL of the supplier.

Case Study Findings

The research found that none of the evaluated contracts include required notification or consent related to terms and conditions modifications.

Table 12: Terms and Conditions Modification Elements in Five North Carolina Public Sector Cloud Contracts

Terms and Conditions Modification Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Notice of Modification					

Recommendations

Many cloud contracts incorporate terms and conditions found at a specified vendor URL. As these can be changed by the supplier at any time, the active terms and conditions at the time of contract signature should be incorporated as an exhibit for future reference purposes. Additionally, the cloud contracts should include provisions related to notice of terms and conditions (T&Cs) modification, particularly if online T&Cs are employed. Ideally, consent by the contracting authority should be required prior to T&C modification, but this rarely occurs in cloud contracts. For example, one contract notes the vendor "may update, amend, modify, or supplement the terms and conditions of this Agreement including the SLA, AUP, and Privacy Policy, from time to time by giving you notice. Such changes will take effect immediately. Any such modification may be made without the consent of any third party beneficiaries of this Agreement." Specifically, we recommend:

- **Recommendation 11:** Contractually obligate the cloud provider to appropriate levels of notification and consent for substantive changes to original contract terms and conditions.

Issue Twelve: Contract Renewal and Termination

Overview

Since switching cloud vendors can be costly and involve significant planning, contract renewal and termination clauses are critically important. This section of a contract identifies what constitutes a renewal or termination of a contract, including what steps must be followed for either option to be legally binding.

Case Study Findings

One of the five contracts allows for the vendor to "terminate the contract for any reason with fifteen (15) calendar days' notice" but requires the governmental entity to "provide 30 days' notice prior to termination." Only one of the five North Carolina cloud contracts includes a non-appropriation provision. Table 13 offers a summary of the contract renewal and termination elements and the findings from the content analysis of the five North Carolina cloud contracts.

Table 13: Contract Renewal and Termination Elements in Five North Carolina Public Sector Cloud Contracts

Renewal and Termination Element Description	Local Government	State Agency	Higher Education	Public Health	K-12
Non-Appropriation Clause	●				
Advance Notice of Contract/Service Termination by Vendor					
Escrow Language	●				

Recommendations

Cloud contracts are similar to all other contracts with respect to the need for specified renewal options and termination clauses. Cloud contracts should specifically state whether automatic renewal will occur unless prior written notice of termination is given, as this is a common practice among cloud providers. Additionally, the contract should state the number of days in advance of renewal the notice of pending termination must be given. Furthermore, the cloud contracts should also mandate the number of days' notice required if the vendor plans to terminate the contract or service. These two clauses should be similar with respect to the number of days of notice, but this is rarely the case if the contract language is not specifically altered by the government customer.

Contracts should include language that allows the customer to terminate the contract without having to show cause as to the reason for termination. Furthermore, governmental entities may be required in certain states to include termination clauses related to non-appropriation of funds. As previously noted, the contract should specify how data will be retrieved/returned upon termination by either party. Escrow language should also be considered in the event of a cloud vendor going out of business, but none of the evaluated contracts include such language. Specifically, we recommend:

- **Recommendation 12a:** Negotiate terms in advance to specify what is required before service can be changed or terminated.
- **Recommendation 12b:** Based on how much notice would be needed to switch to an alternative provider, codify, in the contract, the amount of notice the provider must give before the contract can be terminated.
- **Recommendation 12c:** Restrict termination to triggering events by the customer and provide an opportunity for customer correction before termination can proceed.
- **Recommendation 12d:** Exclude legitimate payment disputes as a reason for provider termination and maintain the right to terminate for cause if the vendor is not able to meet their contractual obligations (Scruggs, Trappler, and Philpott, 2011).

Lessons Learned

Following the evaluation and analysis of the five North Carolina public sector cloud contracts, interviews were conducted with the persons responsible for negotiating each contract to discern unique variations in the contracting environment and to identify the trade-offs made willingly versus those forced by the cloud provider or ignored by the public sector jurisdiction. In all cases, senior-level IT professionals were involved in the cloud contracting process and were included in the interviews. In four of the five cases, the organization's general counsel was also involved in the cloud contracting process and those individuals were also included in the interviews. Three major lessons were ascertained from the interviews with the various participants in the cloud contracting processes.

Lesson One: It is imperative that IT professionals and legal professionals work together to create a technically and legally sound contract.

In many cases, the IT professional would evaluate the contract with limited knowledge of legal issues and perhaps even sign the contract without appropriate legal oversight, thereby exposing the governmental entity to substantial legal risk. In other cases, the legal professional would evaluate the contract solely on legal merits and approve it without a comprehensive understanding of technical issues that may create legal challenges, such as lack of appropriate archiving features in the event of litigation, or an inability to retain data in the event of a litigation hold.

Lesson Two: All contracts, including cloud contracts, are negotiations.

Simply accepting the vendor-supplied master service agreement, service level agreement, acceptable use policy, and/or contract terms is not advisable. Involving key staff from the government, including general counsel, IT experts, and procurement experts, is essential to achieving a contract that will protect the government while ensuring adequate functionality and service.

Lesson Three: All contracts involve some form of risk calculation.

If a government needs or wants a particular cloud service badly enough, or if it deems the risk to be low, then it may be more inclined to accept "click through" contracts, similar to those found on social media sites like Facebook or Twitter. To effectively negotiate a cloud contract with a provider, the organization has to be willing to seek alternative providers or solutions in the event that the government's contract terms cannot or will not be met. This relative risk calculation also requires the governmental entity to have a clear understanding of what contract provisions are must-haves versus nice-to-haves. For example, if a local city ordinance has been passed that specifies non-discrimination in a more restrictive manner than federal or state law, the contract must reflect compliance with that ordinance, hence deeming that provision a must-have.

These three lessons address the need for greater legal education for IT professionals and greater technical education for legal professionals. In fact, the two public sector entities with the greatest number of provisions identified in the assessment framework have legal professionals who specialize in IT-related issues, and also have IT professionals with a basic legal education on procurement laws and public records laws in the state of North Carolina.

Best Practices in Negotiating Cloud Computing Contracts

This study of cloud contracting issues and opportunities in the public sector offers insight into the various challenges facing government units as they navigate the changing tides of cloud computing. Specifically, the research identified and tested a promising practices framework for public sector cloud computing contracts. The comparison of the five contracts against the defined guidelines and requirements creates a baseline understanding of the practical realities facing governments as they negotiate and enter into cloud contracts. Based on our analysis of the case studies and interviews, we found the following best practices:

- **Best Practice One:** Government managers should not simply sign vendor-supplied master agreements, service level agreements, acceptable use policies, and/or contract terms.
- **Best Practice Two:** Government managers should carefully review, negotiate, and modify the terms and conditions of the contract to meet the subscribing organization's needs and legal requirements.
- **Best Practice Three:** Government agencies should employ a collaborative contract negotiation team consisting of experienced information technology, legal, procurement, and business professionals.
- **Best Practice Four:** Government managers should identify which contract provisions are must-haves versus nice-to-haves.
- **Best Practice Five:** Government managers must be willing to seek alternative providers or solutions in the event that the government's contract terms cannot or will not be met.
- **Best Practice Six:** Government agencies should improve legal education for IT professionals, and hire legal professionals with technical expertise. There are a myriad of issues to consider and discuss with legal counsel prior to and during cloud services negotiations. Johndavid Kerr and Kwok Teng sum it up succinctly by saying that "…each organization must conduct a thorough and diligent risk assessment of the potential threats of low to high risk inherent in cloud computing environments, and must ensure that all management and operational strategies and initiatives incorporate an optimal mix of cost-efficient processes, policies, and controls to mitigate against these risks" (2010, p. 19). Each entity must determine which issues are of greatest concern and react accordingly in the hopes of minimizing the potential negative impact of a problem.

Appendix: Methodology

This study addressed the question of how governmental units are managing cloud contracting processes with respect to industry best practices and applicable legal and regulatory requirements. A secondary question addressed is the trade-offs governments are willing to make in order to establish cloud contracts. To address the two main research questions, a multi-stage qualitative process was undertaken. First, the researchers gathered cloud contracts from the five identified North Carolina public sector entities. The five levels of government were selected to ensure that individual variation and legal/regulatory requirements would be addressed in the study as a means to develop a comprehensive framework for cloud contracting for the public sector.

The data analysis process included both deductive and inductive approaches and was conducted in several phases. All five contracts were assessed against the best practices benchmarks generated from legal, academic, and practitioner sources (see Joint and Baker, 2011, Barnes, 2010, and Tufts, 2010) using the qualitative data analysis software QSR NVivo (Version 9). First, the best practices guidelines related to cloud contracts were identified and coded into NVivo. Second, applicable North Carolina and federal laws and regulations that impact contracts in general, and cloud contracts specifically, were identified and coded into NVivo. For both processes, coding definitions were developed to ensure consistent application and reliability.

The five cloud contracts representing different parts of government in North Carolina were read by both members of the research team and coded independently by each researcher. Both pattern-matching and memoing were used as part of the data analysis process. The initial coding structure (best practices and legal/regulatory) was used to analyze each contract, with the research team comparing initial coding of the policies and revising the coding structure based on the common understanding of the main research questions and how this was reflected in the data. All contracts were reviewed again by the researchers and inter-coder reliability was established.

Following the initial stages of cloud contract coding and analysis, interviews were conducted with the persons responsible for negotiating each contract to discern unique variations in the contracting environment and to identify the trade-offs made willingly versus those forced by the cloud provider or ignored by the public sector jurisdiction. Finally, an analysis of the contract issues, decision-making processes, and lessons learned was conducted to provide an appropriate and reasonable framework for developing cloud contracts, while still preserving legal and regulatory requirements, as well as key best practices. This study's research design enabled the research team to collect rich qualitative data on the content of cloud contracts in the five levels of government identified at the onset of the study.

References

Barnes, Frederick R., "Putting a Lock on Cloud-Based Information." *Information Management*, July/August 2010, p. 26–30.

Bradshaw, Simon, Christopher Millard, and Ian Walden. (2011). "Contract for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." *International Journal of Law and Information Technology* 19(3), pp. 187–223.

Cooney, M. (July 11, 2012). The 7 Most Common Challenges to Cloud Computing: U.S. government watchdog group finds common challenges across agencies looking to implement cloud computing but most issues translate into private companies as well. *Network World.* Retrieved from: http://go.galegroup.com.libproxy.lib.unc.edu/ps/i.do?id=GALE%7CA296532126&v=2.1&u=unc_main&it=r&p=AONE&sw=w.

Ernst & Young Global Technology Industry Discussion Series. (2011). Cloud Computing Issues and Impacts. Retrieved from: http://www.ey.com/Publication/vwLUAssets/Cloud-computing_issues_and_impacts/$FILE/Cloud_computing_issues_and_impacts.pdf.

Gatewood, Brent, "Clouds on the Information Horizon: How to Avoid the Storm." *Information Management*, July/August 2009, p. 33–36.

Hogan Lovells, LLP. (2010). Cloud Computing: a Primer on Legal Issues, Including Privacy and Data Security Concerns. Retrieved from: http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/docs/CloudPrimer.pdf.

Joint, Andrew, and Edwin Baker, Knowing the Past to Understand the Present—Issues in the Contracting for Cloud Based Services. *Computer Law and Security Review* 27 (2011), pp. 407–415.

Kerr, J., and K. Teng. (2010). Cloud Computing: Legal and Privacy Issues. Proceedings of the Academy of Business Disciplines Conference. Retrieved from: http://www.g-casa.com/conferences/vietnam/paper/JDK_CLOUDING_9_21_10_Paper-1%5B11%5D.pdf.

Kundra, V. (February 8, 2011). Federal Cloud Computing Strategy. Retrieved from: https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf

Mell, P. and T. Grance. (September, 2011). The NIST Definition of Cloud Computing. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Mills, L.H. (May 13, 2009). Legal Issues Associated with Cloud Computing. Nixon Peabody. Retrieved from: http://www.secureit.com/resources/Cloud%20Computing%20Mills%20Nixon%20Peabody%205-09.pdf.

Tufts, Shannon, "Cloud Contracting: Contract Considerations for Inclusion." UNC School of Government, 2010, available at: http://www.cpt.unc.edu/documents/Cloud_contractV3_000.pdf.

Scruggs, R., T. Trapler, and D. Philpott. (2011). *Contracting for Cloud Services.* Florida: Government Training Inc.

Stevens, G. (April 10, 2012). Data Security Breach Notification Laws. Congressional Research Service. Retrieved from: http://www.fas.org/sgp/crs/misc/R42475.pdf.

United States Government Accountability Office (July 2012). Information Technology Reform: Progress made, but future cloud computing efforts should be better planned. Retrieved from: http://www.gao.gov/assets/600/592249.pdf.

Winkler, V. (May, 2012). Cloud Computing: Legal and Regulatory Issues. *TechNet Magazine.* Retrieved from: http://technet.microsoft.com/en-us/magazine/hh994647.aspx.

Wyld, David, *Moving to the Cloud: An Introduction to Cloud Computing in Government*. Washington, D.C.: IBM Center for The Business of Government, 2009.

About the Authors

Shannon Howle Tufts, Albert and Gladys Coates Distinguished Term Assistant Professor of Public Law and Government, is the Director of the University of North Carolina at Chapel Hill School of Government's Center for Public Technology. She works with local IT directors and staff on a variety of technology-related issues, including designing and instructing in the first local and state government-specific CIO Certification Programs in the nation. She also teaches in the Masters of Public Administration program, focusing on strategic information technology investments, research methods/statistics, and program evaluation. Her research efforts center on the public sector's use of information technology, particularly the human factors associated with IT implementation. She has a PhD from North Carolina State University.

Meredith Leigh Weiss is the Associate Vice Chancellor for Business Services and Administration at the University of North Carolina at Chapel Hill and adjunct assistant professor at the UNC's School of Information and Library Science. Additionally, she teaches for several online executive MBA and PhD programs across the country. Her academic interests include information technology management and leadership, evidence-based management, business analytics, human resources, instructional technology, and distance education.

Weiss earned her bachelor's degree in human resources from the University of Delaware, has Master of Business Administration and Master of Information Science degrees from North Carolina Central University, holds a Master of Science in instructional technology and certificate in distance learning and administration from East Carolina University, and received a Ph.D. in information science from the University of North Carolina at Chapel Hill's School of Information and Library Science.

Key Contact Information

To contact the authors:

Shannon H. Tufts, PhD
Albert and Gladys Hall Coates Assistant Professor and Director, Center for Public Technology
School of Government
University of North Carolina at Chapel Hill
CB#3330 Knapp-Sanders Building
Chapel Hill NC 27599
(919)962-5438 (office)

e-mail: tufts@unc.edu

Meredith Weiss, PhD
Associate Vice Chancellor for Business Services and Administration
Division of Finance and Administration
University of North Carolina at Chapel Hill
South Building
Campus Box 1000
Chapel Hill, NC 27599-1000
(919) 843-4080

e-mail: mlweiss@email.unc.edu

Reports from IBM Center for The Business of Government

For a full listing of IBM Center publications, visit the Center's website at **www.businessofgovernment.org.**

Recent reports available on the website include:

Acquisition

A Guide for Agency Leaders on Federal Acquisition: Major Challenges Facing Government by Trevor L. Brown
Controlling Federal Spending by Managing the Long Tail of Procurement by David C. Wyld

Assessing the Recovery Act

Recovery Act Transparency: Learning from States' Experience by Francisca M. Rojas
Key Actions That Contribute to Successful Program Implementation: Lessons from the Recovery Act by Richard Callahan, Sandra O. Archibald, Kay A. Sterner, and H. Brinton Milward
Managing Recovery: An Insider's View by G. Edward DeSeve
Virginia's Implementation of the American Recovery and Reinvestment Act: Forging a New Intergovernmental Partnership by Anne Khademian and Sang Choi

Collaborating Across Boundaries

Collaboration Between Government and Outreach Organizations: A Case Study of the Department of Veterans Affairs by Lael R. Keiser and Susan M. Miller
Using Crowdsourcing In Government by Daren C. Brabham
Developing Senior Executive Capabilities to Address National Priorities by Bruce T. Barkley, Sr.
Beyond Citizen Engagement: Involving the Public in Co-Delivering Government Services by P. K. Kannan and Ai-Mei Chang
Implementing Cross-Agency Collaboration: A Guide for Federal Managers by Jane Fountain

Fostering Transparency and Democracy

Assessing Public Participation in an Open Government Era: A Review of Federal Agency Plans by Carolyn J. Lukensmeyer, Joe Goldman, and David Stern

Improving Performance

Predictive Policing: Preventing Crime with Data and Analytics by Jennifer Bachner
The New Federal Performance System: Implementing the GPRA Modernization Act by Donald Moynihan
The Costs of Budget Uncertainty: Analyzing the Impact of Late Appropriations by Philip G. Joyce

Using Technology

Rulemaking 2.0: Understanding and Getting Better Public Participation by Cynthia R. Farina and Mary J. Newhart
The Use of Data Visualization in Government by Genie Stowers
Mitigating Risks in the Application of Cloud Computing in Law Enforcement by Paul Wormeli
Challenge.gov: Using Competitions and Awards to Spur Innovation by Kevin C. Desouza
Working the Network: A Manager's Guide for Using Twitter in Government by Ines Mergel

IBM Center for
The Business of Government

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit: ibm.com

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342
website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.