Service Level Agreements for IT

Sunday, May 22, 3:50 – 4:40, CPE - 1

Linda Cramer, Assistant County Manager, Chatham County
Gary Robinson, Director Budget and Finance, Pierce County
Todd Sander, Executive Director, Center for Digital Government
Service-Level Agreements for IT

Todd Sander
Executive Director
Center for Digital Government
Best Practice Guide for Cloud and As-a-Service Procurements started with CDG through its Digital Performance Institute and Digital Communities Program

Brought together public and private sector leaders to create a guide that would identify potential improvements to procurement policies

Working with Delaware’s “Cloud First Policy” the group shared ideas and perspectives on terms and conditions related to SaaS, PaaS
Government and Industry Working Together

Cloud-as-a-Service

- **Software-as-a-Service (SaaS)**
  Cloud-hosted Software Services that are purchased

- **Platform-as-a-Service (PaaS)**
  Cloud-hosted Services that are deployed

- **Infrastructure-as-a-Service (IaaS)**
  Cloud-hosted Services that are built

© 2016 e.Republic
Understand What You Are Buying

Public Sector Management of XaaS Platforms

<table>
<thead>
<tr>
<th>Traditional IT</th>
<th>Infrastructure (as a Service)</th>
<th>Platform (as a Service)</th>
<th>Software (as a Service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
</tr>
<tr>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
</tr>
<tr>
<td>Operating System</td>
<td>Operating System</td>
<td>Operating System</td>
<td>Operating System</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
</tr>
</tbody>
</table>

You manage, Delivered as a service

Source: Adapted from IDC Government Insights

© 2016 e.Republic
Examples in Cloud Computing

- **Software-as-a-Service (SaaS)**
  - E-mail, Business Processes, CRM, ERP, HR
  - Office 365, Salesforce, NetSuite

- **Platform-as-a-Service (PaaS)**
  - Middleware, Development Tooling
  - Windows Azure, force.com, Java Runtime

- **Infrastructure-as-a-Service (IaaS)**
  - Servers, Networking, Storage
  - VM Ware, Amazon Web Services, OpenStack
Drivers in Cloud Computing

- Collaboration
- Business Agility
- Decreased Costs
Developing Trends

### 2015 Digital Cities Survey

- **In use currently**: 51%
- **Will upgrade / expand / replace in 18-25 months**: 29%
- **May start using in 18-24 months**: 12%

### 2015 Digital Counties Survey

- **In use currently**: 39%
- **Will upgrade / expand / replace in 18-24 months**: 20%
- **May start using in 18-24 months**: 23%
# Developing Trends

2014 Digital States Survey, Cloud Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>In use currently</th>
<th>Plans to implement G2G/private</th>
<th>Plans to implement 3rd party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Resource Planning (ERP)</td>
<td>32%</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>Customer Relationship Management (CRM)</td>
<td>55%</td>
<td>11%</td>
<td>23%</td>
</tr>
<tr>
<td>E-mail</td>
<td>64%</td>
<td>19%</td>
<td>19%</td>
</tr>
</tbody>
</table>
Perception Matters

2016 Public Administration Governing Exchange Survey

When asked whether they believe risk is greater when procuring cloud (XaaS) services than with traditional vendor services:

- 23% believe risk is increased
- 25% believe risk is not increased
- 52% did not know
Developing Trends

2016 Public Administration Governing Exchange Survey

- Where are the areas of increased risk in procuring XaaS?
- Why is there no increased risk?

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data and Information Security</td>
<td>88%</td>
</tr>
<tr>
<td>Vendor Stability and Reliability</td>
<td>51%</td>
</tr>
<tr>
<td>System Governance And Data Ownership</td>
<td>49%</td>
</tr>
<tr>
<td>Safeguards in Place</td>
<td>58%</td>
</tr>
<tr>
<td>All IT Equally Risky</td>
<td>37%</td>
</tr>
<tr>
<td>Managing Cloud As Routine</td>
<td>21%</td>
</tr>
</tbody>
</table>
Why Service Level Agreements Matter

Key Points to Watch For

- Technical service level performance promises
- Description of service quality
- Identification of roles and responsibilities
- Security responsibilities and notice requirements
- How disputes are discovered and addressed
- Remedies for performance failures
- Risk
## Important Details to Include

- Service provider and the public jurisdiction must agree to the specific details of service.
- These should be specific in the T&Cs and SLA.

### Best Practices in T&Cs and SLA

<table>
<thead>
<tr>
<th>1</th>
<th>Service Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Data</td>
</tr>
<tr>
<td>3</td>
<td>Personnel</td>
</tr>
<tr>
<td>4</td>
<td>Security and Breach Notification</td>
</tr>
<tr>
<td>5</td>
<td>Audits</td>
</tr>
<tr>
<td>6</td>
<td>Operations</td>
</tr>
</tbody>
</table>
Data

Ownership

• Governments have a responsibility to limit access to non-public information and to protect the integrity of their data (clause 1, 2 and 3)

Location

• Service providers are required to provide services only from data centers located within the US (clause 4)

Import and Export

• Public jurisdictions are allowed the ability to import and/or export its data in a whole or in part at their sole discretion (clause 16)
Security

Logs and Reports

• Service provider is required to provide reports of user access history and security logs for the data under the contract (clause 10)

Encryption of Data at Rest (Mobile Devices)

• Service provider is required to prevent its employees from storing personal data on portable devices (clause 23)

Breach Notification

• Requires service provider to notify the jurisdiction of a data breach, notify the jurisdiction when it receives a request for access of data, and to return all jurisdiction data in an orderly time (clause 5, 7, 8)
Responsibility and Uptime Guarantee

- Service provider is responsible for all of the plant, capacity, hardware, software and personnel needed to provide the service 24/7 (clause 17)

Changes and Maintenance

- Service provider is required to give advance notice of upgrades or system changes (clause 13)

Operations Business Continuity and Disaster Recovery

- Requires a business plan and disaster recovery plan for the service provider’s operations (clause 20)
Best Practices in T&Cs and SLA

Points to Consider

- Understanding Shared and Managed Risk
- Realistic Assessment of Risks
- Consider a Variety of Risk Management Alternatives
Thank You!

Todd Sander
Executive Director
Center for Digital Government
tsander@erepublic.com
916-932-1373
Service Level Agreements

May 22, 2016
Pierce County Characteristics

- Pierce County is the second largest county in Washington State.
- Land area 1,794 square miles from sea level at Puget Sound to 14,411 feet at the peak of Mt. Rainier.
- Seattle is 35 miles north. Olympia is 30 miles south.
- Population over 814,600.
- Annual total funds budget $903 Million.
- 3,000 Full Time Staff.
- Site of the 2015 U.S. Open Golf Championship.
Contracts

Software as a Service

• Applications, Data, Middleware, Operating System, Servers, Storage, Networking

Pierce County Services

• Seventy-One Services, Including Financials, Human Resources, Web Site, Social Media, Electronic Mail, Office, and Data Storage
Contracts

Service Level Agreements

• Contracts with Company or other Provider (Internal or External) for Purchase or Use of Software, Hardware, or Services.

Cloud Solutions Focus on Use

• Contractor grants Customer a non-exclusive, non-transferable, right to use the service solely for the internal business purposes during the term, and conditions of agreement within scope of use defined in the order form.
Provisions

Functionality / Requirements

• Scope
• Change and Configuration
• Event Management

Usage License

• Contractor and Customer Responsibilities
Provisions

Term – Survivorship – Escrow

Data – Information Life Cycle

• Collection, Storage/Retention, Destruction
• Access
• Integrity
• Backups
• Ownership – Customer, Aggregate, and Statistical Records
Provisions

Data – Information Life Cycle

• Contractor owns the aggregated and statistical data derived from the operation of the Service.

• Parties shall not disclose or use any confidential information of the other party.

• Each party agrees to protect confidential information of the other party.

• If a party discloses or uses confidential information of the other party in breach of confidentiality protections, the other party shall have the right to seek injunctive relief to enjoin such acts.

• Contractor recognizes that Customer is a public agency subject to public information laws.
Provisions

Data – Information Life Cycle

- Upon request of Customer made within thirty (30) days after expiration of agreement, Contractor will make Customer Data available to Customer through the Service on a limited basis solely for purposes of Customer retrieving Customer Data for a period of up to thirty (30) days after such request is received by Contractor.
Service Operation–Performance Requirements

• Uptime and Responsiveness
• Updates and Capacity Monitoring

Response commitment is (i) not less than 50% of online transactions in 2 seconds and (ii) not more than 10% in 5 seconds or more. Service Response is the processing time of the Contractor production data center to completer transactions submitted from a web browser.
Provisions

Case Submittal and Reporting

• Response and Escalation
• Severity Level Determination
• *Customer shall reasonably self-diagnose each support issue and recommend to Contractor an appropriate Severity Level designation. Contractor shall validate Customer’s Severity Level designation, or notify Customer of proposed change.*
Provisions

Case Response – One to Four Hours

- **Severity Level 1** – Service is unavailable for all users or issue prevent processing.
- **Severity Level 2** – Service contains a bug that prevents Customer from executing one or more critical business processes with a significant impact and no workaround exits.
- **Severity Level 3** – Service contains a bug that prevents Customer from executing one or more important business processes and a work around exists, but is not optimal.
- **Severity Level 4** – Service contains an issue that may disrupt important business processes where a work around is available or functionality is not imperative to business operations.
- **Severity Level 5** – Non-system issues.
Provisions

Compliance with Standards

• Security – Awareness, Access, Physical and Environmental, Incident Response, Audits

• *Contractor shall maintain a formal security program in accordance with industry standards to: (i) ensure the security and integrity of Customer Data; (ii) protect against threats or hazards to Customer Data; and (iii) prevent unauthorized access to Customer Data.*
Provisions

Compliance with Standards

• Health Insurance Portability and Accountability Act
• Payment Card Industry Data Security Standards for Credit Card Use
Contingency Planning and Disaster Recovery

• Contractor shall implement and maintain a business continuity and disaster recovery plan that provides for the continued delivery of the Service in the event of a power outage, systems outage, or other circumstances that may interrupt the normal provision of the Services.
Provisions

Disputes and Remedies
  • Service Credits

Contract Manager
  • Service Delivery and Performance Monitoring
  • Payment Authorization
  • Risk Management
  • Issue Resolution
Questions?

Thank You!