CAPPO

California Association of Public Procurement Officials, Inc.

Established 1915

106TH ANNUAL CAPPO CONFERENCE & SUPPLIER EXPO

Contracting in the Cloud

Mike Mucha, GFOA

A Professional Organization Dedicated to the Support and Education of California's Procurement Officials

Agenda Topics

- What is the cloud and how do you buy it?
- Role of procurement
- Common issues and risks
- Approaches for:
  - Setting expectations for RFPs
  - Contract negotiations

What is the cloud?

Common Terms

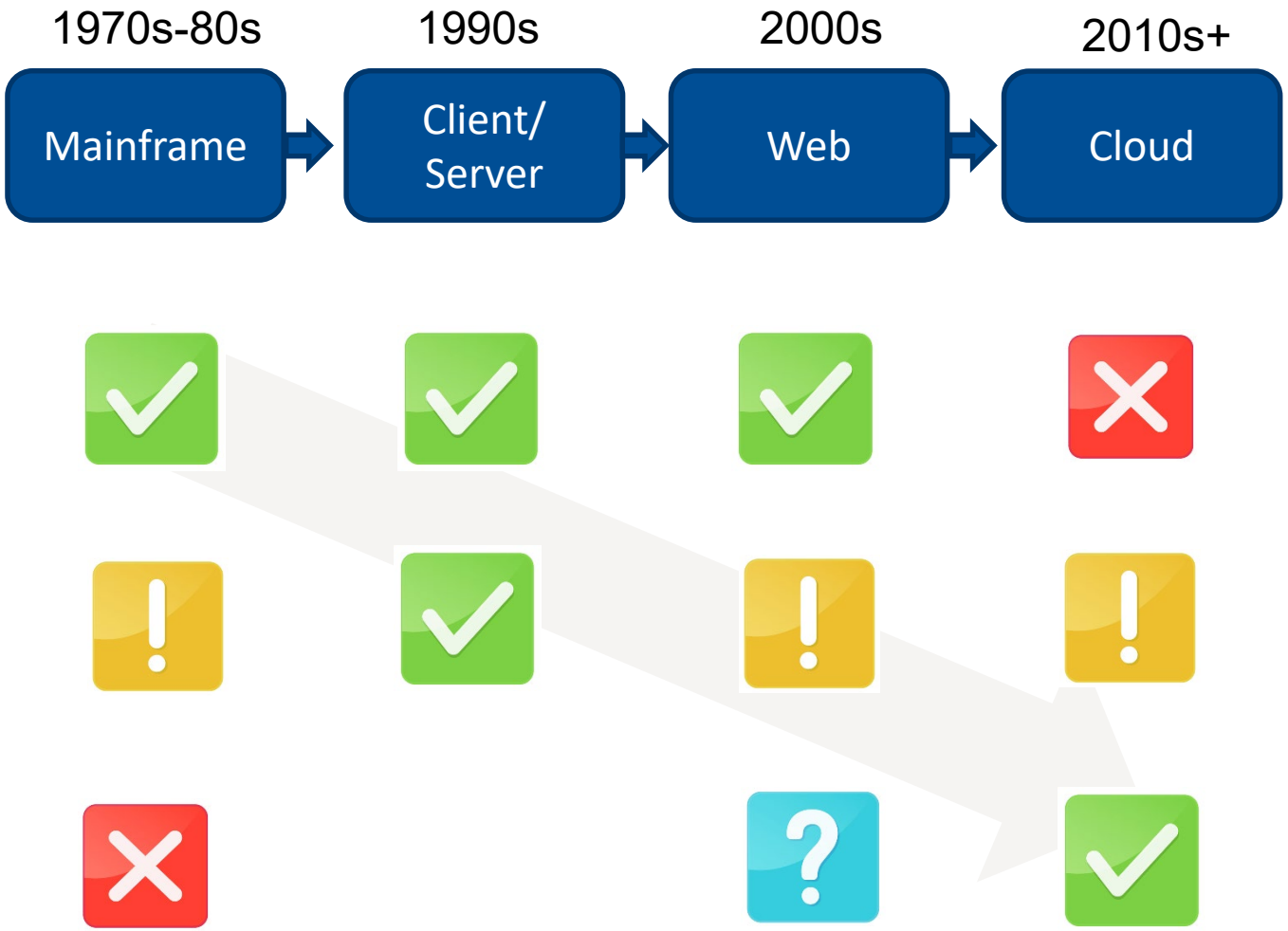
- **Cloud computing** – on-demand access via the internet to computing resources
  - Infrastructure-as-a-service (IaaS
  - Platform-as-a-service (PaaS)
  - Software-as-a-service (SaaS

- **Multi-tenant / Single-tenant**
- **Public cloud / Private cloud**
- **Hybrid cloud**
- **Internet of things (IoT)**
- **Microservices**

SaaS vs. Cloud

- Not all “clouds” are the same
  - Every vendor will use a slightly different model for:
    - Licensing software
    - Providing support
    - Deploying upgrades
    - Using third party vendors

Evolution of Software



Adoption in public sector has met resistance, but cloud has many advantages

- Governments core competency is not server administration
- Managed risk
- Allow for more powerful products and sophistication without large IT departments

Cloud = Outsourcing

- Vendor has advantage from ability to specialize and economies of scale
  - Specialized security administration
  - Ability to recruit staff with specialized skillsets
- Customer (government) compensates vendor for providing services and for transfer of risk
  - Risk on vendor for performing services up to service level standard
  - Requires service level standards / service level agreements (SLAs)

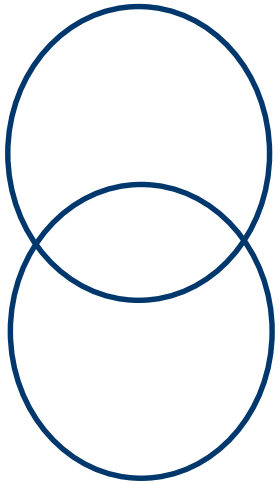
Cloud procurement requires strategic focus

- Outcome focused specifications
- Improved analysis
  - Cost benefit
  - Risk analysis
  - Business case
  - Long-term costs costing / Indirect impacts
- Better coordination
  - Improved competition
  - Enterprise approach to contracting
  - Strategic use of network outside of government

Basics of Cloud Procurement

Cloud Procurement has 2 sides

- Application (software)
  - Functional fit
  - Business process optimization
  - Reporting
  - Role security
- Infrastructure
  - Availability
  - Integration
  - Performance
  - Physical and technical security



Key Elements of Software Procurement

- Functional requirements are essential
  - Well defined project goals are required for project success
- Focus on business process and business outcomes
  - Focus on configured / delivered system
  - Technology is the tool
- Major system implementations are more about organizational change than technology
- Need to hold vendor accountable for scope and quality

Technology is NOT the hard part

- Software vendors provide robust functionality and broad product suite to meet government needs
- Software capable of meeting government needs
- Governments continue to struggle with implementation
  - Change in process
  - Modernize
  - Changing organizational roles
  - Project accountability
  - Realization of improved outcomes

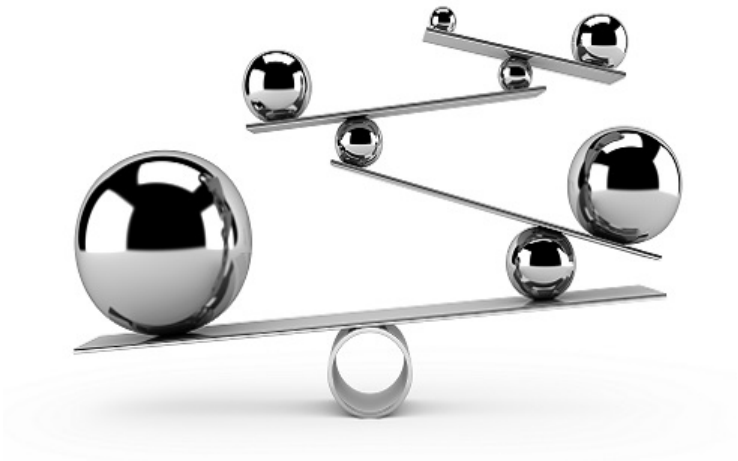
Procurement of cloud “infrastructure” is about understanding risk

- Service level agreements (SLAs)
- Business continuity
- Risk mitigation
- Liability

Role of Procurement

Why procurement?

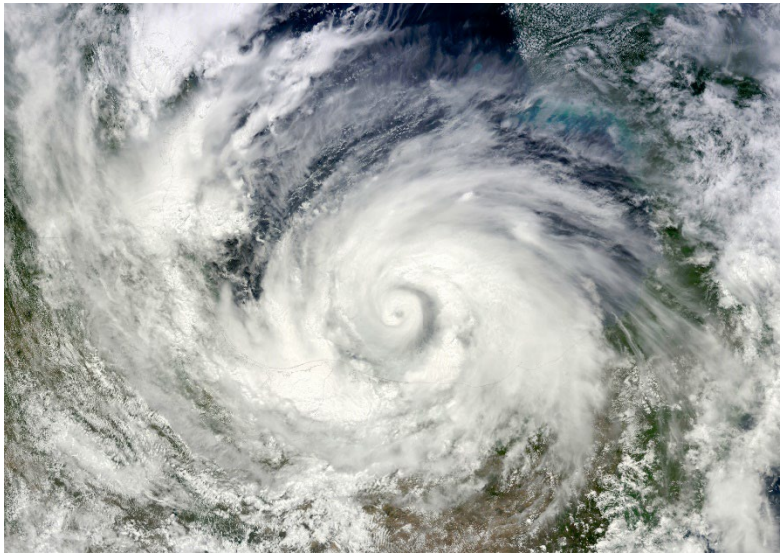
- Ethics
- Compliance
- Efficiency
- Fairness
- Analysis
- Transparency
- Coordination / Customer Service
- **Performance / Accountability**
- **Business Continuity / Risk Mitigation**



What could go wrong?

What could go wrong?

What could go wrong?



What could go wrong in this “cloud”?

What could go wrong?

- How much will it hurt?
- How much control do we really have?
  - What is expectation of control?
  - How much interaction / dependency?

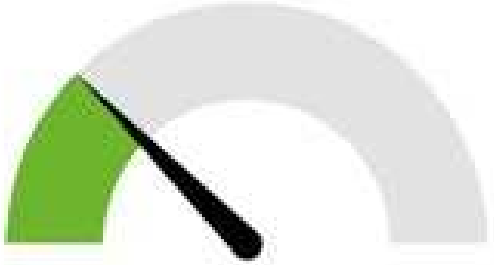
Key Issues in Cloud Procurement

Overall Assessment for Public Sector

- Technology is mature
- Contract norms are not
- Risk:

Price

Software Fit



Vendor Risk

Government Risk

Would you sign this?

Organization acknowledges and agrees that use of or connection to the Internet is inherently insecure and provides opportunity for unauthorized access by a third party to Organization's and its Users' (as well as Vendor's) computer systems, networks and any and all information stored therein. Organization is solely responsible for making an independent determination as to whether the technical and organizational measures for the Services meet Organization's requirements, including any and all of its security obligations under applicable Data Protection Requirements

Key Issues

- Contract structure
  - Price
- Control of data
- Service level agreement (availability / performance)
- Security / Liability

SaaS Contracts (common expectations)

- Multi-year Agreements
  - 6-10 years
- Fixed pricing
  - Flat pricing / year or slight adjustments
- Termination is very difficult
- You do not have ability to reduce level of service

- Potential for price increases for violating license subscription terms
- What is not included in your agreement?

Examples (license metrics)

- "Full-Time Employee" is an employee of Customer regularly scheduled for more than twenty hours per week

- Hosted Employee: is defined as
  - all of your full-time, part-time, temporary employees, and
  - all of your agents, contractors and consultants who have access to, use of, or are tracked by, the programs. The quantity of the licenses required is determined by the number of Hosted Employees and not the actual number of users.
  - In addition, if you elect to outsource any business function(s) to another company, the following must be counted for purposes of determining the number of Hosted Employees: all of the other company's full-time employees, part-time employees, temporary employees, agents, contractors and consultants that (i) are providing the outsourcing services and (ii) have access to, use of, or are tracked by, the programs.

How do you know what you are buying?

- Scenario:
  - You license procurement module for use with 12 named users.
- Problem:
  - What does the procurement module do?
  - Is contract management in a separate module?
  - P-cards?
  - Do department users need a license to enter requisitions?

Data Ownership

- Data are owned by government

- Can you get the data back?
- What can the vendor do with your data?

Would you sign this?

Customer Data

Customer retains all right, title, and interest in the Customer Data and all Intellectual Property Rights therein. Customer hereby grants to VENDOR a non-exclusive, royalty-free license to, and permit its partners (which include, without limitation the hosting providers of the Software Services) to, use, store, edit and reformat the Customer Data, and to use Customer Data for purposes of sales, marketing, business development, product enhancement, customer service, or for analyzing such data and publicly disclosing such analysis, provided that in all such uses Customer Data is rendered anonymous such that Customer is no longer identifiable.

Customer may download the Customer Data from the Software Services at any time during the Term, other than during routine software maintenance periods. VENDOR has no obligation to return Customer Data to Customer.

Service Level Agreements need to be documented

- Availability
- Back-ups
- Restore time
- Issue response
- Security audits
- Reporting of SLA

- What happens is SLA is missed?

Example SLAs

Example 1

$$\left(\frac{\text{Total} - \text{Unplanned Outage} - \text{Planned Maintenance}}{\text{Total} - \text{Planned Maintenance}}\right) \text{X } 100\% \geq 99.7\%$$

Example 2

Would you sign this?

The percentage of time the Software is available during a calendar quarter, with percentages rounded to the nearest whole number.

Targeted Attainment	Actual Attainment	Client Relief
100%	98-99%	Remedial action will be taken.
100%	95-97%	4% credit of fee for affected calendar quarter will be posted to next billing cycle
100%	<95%	5% credit of fee for affected calendar quarter will be posted to next billing cycle

How much is too much?

- 31 days = 744 hours = 44,640 minutes

% Available	Allowable Downtime
99.99%	4.5 minutes
99.9%	44.6 minutes
99%	7.4 hours
97.5%	18.6 hours
95%	37.2 hours
90%	74.4 hours

Be careful of SLA comparison for quarter.
Downtime for quarter is 3X that for month.

Security and the Cloud

- Local governments are more likely to be the targets of a ransomware attack than any other kind of organization

- What could go wrong:
  - Ransomware
  - Breach of information
  - Loss of data
  - Inability to provide service

Scenario: Ransomware attack with popular cloud SaaS vendor

- Vendor became aware of ransomware attack
- 2,000 customers lost access to the system and for a long time (month)
  - Business continuity
  - Disruption after service has been restored
- Reputational hit
  - **Was vendor down or were you down?**
    - **Employees, vendors, citizens are all impacted**
    - **Who is responsible?**

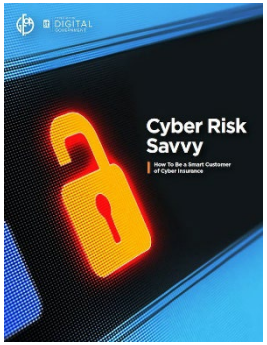
Vendors often limit liability which puts the government at risk

- Limitation of Liability
  - $ limits
  - Exclusion of damages

- No specific protections for breach of personal or payment information
- Suspension of service
- Termination of contract

Who is responsible for breach?

- Standard vendor limitation of liability is set at amount equal to fees paid in last 12 months.
- Need to understand responsibility under law for breach of personal information
- PCI compliance
- Cyber insurance may not be a reliable option
  - Recent volatility in pricing
  - Exclusions exist in all policies



https://www.gfoa.org/cyber-insurance

Strategies for RFP

Procurement Protections for Cloud

- Define clear requirements
  - Don’t rely on industry standard assumptions
- Set clear SLAs with appropriate penalties
- Fully understand preventative measures to protect against loss
  - Test procedures and audit vendors
- Insist on appropriate risk transfer
- Consider full costs of service

Additional Information

https://www.gfoa.org/cappo

Contact information :

Mike Mucha
Deputy Executive Director
Government Finance Officers Association
Phone: 312.977.9700
Direct: 312.578.2282
mmucha@gfoa.org